

JAPAN PATENT OFFICE



This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: October 4, 2001

Application Number: Patent Application
 No. 2001-308387

Applicant(s): FUJITSU LIMITED

October 26, 2001

Commissioner,
Japan Patent Office Kozo OIKAWA

Certificate No. 2001-3093372

BEST AVAILABLE COPY

日 本 国 特 許 庁
JAPAN PATENT OFFICE



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application:

2001年10月 4日

出 願 番 号
Application Number:

特願2001-308387

出 願 人
Applicant(s):

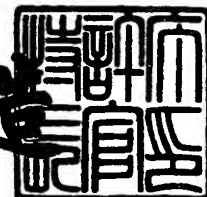
富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年10月26日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3093372

【書類名】 特許願

【整理番号】 0151680

【提出日】 平成13年10月 4日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 13/00

【発明の名称】 パケット中継処理装置

【請求項の数】 20

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 嶋田 邦昭

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 横山 乾

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 栗田 敏彦

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 勝山 恒男

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 川崎 健

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

株式会社内
【氏名】 高場 浩一
【発明者】
【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通
株式会社内
【氏名】 ▲蔭▼山 博靖
【特許出願人】
【識別番号】 000005223
【氏名又は名称】 富士通株式会社
【代理人】
【識別番号】 100074099
【住所又は居所】 東京都千代田区二番町 8 番地 2 0 二番町ビル 3 F
【弁理士】
【氏名又は名称】 大菅 義之
【電話番号】 03-3238-0031
【選任した代理人】
【識別番号】 100067987
【住所又は居所】 神奈川県横浜市鶴見区北寺尾 7 - 2 5 - 2 8 - 5 0 3
【弁理士】
【氏名又は名称】 久木元 彰
【電話番号】 045-573-3683
【先の出願に基づく優先権主張】
【出願番号】 特願2001- 90122
【出願日】 平成13年 3月27日
【手数料の表示】
【予納台帳番号】 012542
【納付金額】 21,000円
【提出物件の目録】
【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9705047

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 パケット中継処理装置

【特許請求の範囲】

【請求項 1】 ネットワーク接続装置を有するパケット中継処理装置であって、

上記ネットワーク接続装置がセッションを管理するセッション管理部と、

上記セッション管理部によるセッション管理に基づいてパケットを中継するパケット処理部を備えている

ことを特徴とするパケット中継処理装置。

【請求項 2】 上記ネットワーク接続装置は、更に、上記パケットのルーティング先に関するルーティング情報を格納するルーティングテーブルと、

上記セッションの開始時に、上記ルーティング情報に基づいて上記パケットのルーティング先を決定するルーティング処理部を更に備え、

上記パケット処理部は、上記パケットを決定された上記ルーティング先に出力する、

ことを特徴とする請求項 1 に記載のパケット中継処理装置。

【請求項 3】 上記パケット中継処理装置は、更に、サーバを備え、

上記サーバは、上記ルーティングテーブルに上記ルーティング情報を書き込むネットワーク制御部を備える、

ことを特徴とする請求項 2 に記載のパケット中継処理装置。

【請求項 4】 上記パケット中継処理装置は、さらに、サーバを備え、

上記サーバは、上記セッションを管理する外部セッション管理部を備え、

上記セッション管理部は、与えられた条件に応じて上記セッションに関するセッション情報を上記サーバに転送し、

上記外部セッション管理部は、受信した上記セッション情報に基づいて上記セッションを管理する、

ことを特徴とする請求項 1 に記載のパケット中継処理装置。

【請求項 5】 上記ネットワーク接続装置は、更に処理振分部と複数のサービス処理部を備え、

上記処理振分部は、上記パケットに対するサービスの内容に基づいて、上記複数のサービス処理部のうち少なくとも1つに上記パケットを振り分け、

上記パケットを振り分けられたサービス処理部は、上記パケットに対するサービス処理を実行する、

ことを特徴とする請求項1に記載のパケット中継処理装置。

【請求項6】 上記パケット中継処理装置は、更にサーバを備え、

上記サーバは、外部サービス処理部を備え、

上記処理振分部は、与えられた条件によって、上記パケットを上記サーバに転送し、

上記外部サービス処理部は、受信したパケットに対するサービスを実行する、ことを特徴とする請求項5に記載のパケット中継処理装置。

【請求項7】 上記パケット中継処理装置は、サーバを更に備え、

上記サーバは、パケット詳細解析部を備え、

上記ネットワーク接続装置は、更に処理振分部とサービス処理部を備え、

上記処理振分部が、与えられた条件によって上記パケットを上記パケット詳細解析部に転送し、

上記パケット詳細解析部は、上記パケットを解析することにより上記パケットに対するサービス内容を決定し、決定した上記サービス内容を上記ネットワーク接続装置に設定し、

上記設定後、上記ネットワーク接続装置は、上記決定されたサービス内容に基づいて上記パケットを処理する、

ことを特徴とする請求項1に記載のパケット中継処理装置。

【請求項8】 上記ネットワーク接続装置は、上記セッションに関するセッション情報を格納するセッションテーブルと、上記パケットに対するサービスを実行するための規則を記述するポリシーを格納するポリシーテーブルを備え、

上記セッション管理部は、上記パケットを受信した場合、上記パケットに含まれる情報を検索キーとして用いてセッションテーブルを検索し、

上記検索の結果、該当するセッション情報が上記セッションテーブルに登録されていない場合には、上記セッション管理部は、さらに上記パケットに含まれる

情報を検索キーに基づいて、上記ポリシーテーブルから上記ポリシーを取得し、上記取得したポリシーに基づいて、上記セッション情報を上記セッションテーブルに書き込み、

上記検索の結果、該当するセッション情報が上記セッションテーブルに登録されている場合には、上記セッション管理部は、上記セッションの状態に基づいて、上記セッションテーブルに格納されたセッション情報を管理することを特徴とする請求項 5 又は請求項 6 に記載のパケット中継処理装置。

【請求項 9】 上記パケット中継処理装置はサーバを備え、

上記サーバは、上記ポリシーを上記ポリシーテーブルに書き込むサービス制御部を備える、

ことを特徴とする請求項 8 に記載のパケット中継処理装置。

【請求項 10】 上記セッション管理部は、更に、上記セッションが終了してから所定時間経過した後に、上記終了したセッションに関するセッション情報を上記セッションテーブルから削除することを特徴とする請求項 1 乃至請求項 9 いずれか 1 項に記載のパケット中継処理装置。

【請求項 11】 上記ネットワーク接続装置は、更に、パケットに関する統計情報を取得するためのカウンタを備えることを特徴とする請求項 1 乃至請求項 10 のいずれか 1 項に記載のパケット中継処理装置。

【請求項 12】 複数のポリシーは複数のグループに分けられ、

上記ネットワーク接続装置は、更に、上記グループ毎に各ポリシーが有効であるか否かを設定することを特徴とする請求項 8 又は請求項 9 に記載のパケット中継処理装置。

【請求項 13】 上記ネットワーク接続装置は、更に、上記パケットのログを採取するために、上記パケットの少なくとも一部を上記サーバに転送することを特徴とする請求項 9 に記載のパケット中継処理装置。

【請求項 14】 上記セッション情報は、上記サーバに上記パケットを転送すべきか否かを示すサーバ転送指示情報を含み、上記処理振分部は、上記サーバ転送指示情報に基づいて、上記パケットを上記サーバへの転送を行うか否かを決定する事を特徴とする請求項 9 に記載のパケット中継処理装置。

【請求項15】 上記パケット詳細解析部は、更に、上記サーバに転送された上記パケットがHTTPプロトコルのGETパケットである場合、上記パケットに含まれるURL (Uniform Resource Locator) に基づいて、上記パケットに対するサービスを決定する、
ことを特徴とする請求項7に記載のパケット中継処理装置。

【請求項16】 上記パケット詳細解析部は、更に、上記サーバに転送された上記パケットがFTPプロトコルのPORT命令、或いはPASV命令のACKである場合、上記セッションのデータコネクションのIPアドレスとポート番号に基づいて、上記パケットに対するサービスを決定する、
ことを特徴とする請求項7に記載のパケット中継処理装置。

【請求項17】 上記パケット詳細解析部は、上記サーバの負荷を分散させる処理を行う場合、上記負荷の振分先となる振分先サーバが決定されるまで、上記振分先サーバに代わって応答することを特徴とする請求項7に記載のパケット中継処理装置。

【請求項18】 上記パケット詳細解析部は、上記パケットを解析することにより、上記セッションテーブルに、上記パケットに対するサービスの種類、変換用IPアドレス及びポート番号、シーケンス番号及びACK番号差分を書き込む、
ことを特徴とする請求項7に記載のパケット中継処理装置。

【請求項19】 パケット中継処理装置におけるネットワーク接続装置であって、

上記ネットワーク接続装置がセッションを管理するセッション管理部と、
上記セッション管理部によるセッション管理に基づいてパケットを中継するパケット処理部を備えている
ことを特徴とするネットワーク接続装置。

【請求項20】 パケットを中継する制御を、ネットワーク接続装置に備えられたコンピュータに実行させるプログラムであって、
セッションを管理し、
上記セッション管理に基づいて上記パケットを中継する

ことを含む処理を上記コンピュータに実行させることを特徴とするプログラム

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、サーバ負荷分散制御、NAT (Network Address Translation)、帯域制御、VPN (Virtual Private Network)、ファイアウォールサービス機能を持ったサーバを最適化するためのパケット中継処理装置に関する。

【0002】

【従来の技術】

現在、WWW (World WideWeb) やE-mail、携帯電話におけるパケット通信サービスの普及により、インターネットが急速に大規模化している。それに伴い、ネットワークのさらなる高速化や、セキュリティ等の高機能化の要求が高まって来ている。現状のネットワークサービスの実行形態は、サーバと、NIC (NetworkInterface Card) 等のネットワーク接続装置という構成が一般的である。昨今のネットワークサービスは複雑化してきており、様々な、そして新しい要求に対し柔軟に対応できるという点で、サーバというプラットフォームが適している。

【0003】

図39に従来のパケット中継処理装置の構成を示す。同図はサーバとネットワーク接続装置がネットワーク上で、サービスを実現する一般的な構成を示しており、矢印は制御情報の流れ、太い矢印はパケット情報を示す。

【0004】

同図において、100はサーバであり、パケット処理部101と、サービス1処理部～サービスn処理部102と、サービス1制御部～サービスn制御部103を備える。

【0005】

サービス1処理部～サービスn処理部102は、サービス1制御部～サービスn制御部103で定めるポリシーに従い、セッション管理やルーティングを行う

とともに、フィルタリングや負荷分散等のサービス処理を行う。

【0006】

104はネットワーク接続装置であり、ネットワーク接続部を介してネットワークから入力されたパケットは、ネットワーク接続装置104、パケット通信部105を介してサーバ100のパケット処理部101に送られ、パケットが処理される。

【0007】

【発明が解決しようとする課題】

最近の急激なインターネットの大規模化のため、ネットワークを流れるパケットの量は指数関数的な伸びを示している。このため、従来のサーバでは、要求される処理速度に 대응できなくなっており、サーバを高速化する技術が求められている。また、新しいプラットフォームを作る上で、サーバの多くのサービスを統合することができるという点は、できる限り損なわないようにしたい。

【0008】

本発明は上記問題を解決するためになされたものであって、多くのネットワークサービスで使用している共通処理を、ネットワーク接続装置に配置することにより、サーバのサービス処理を高速化することを目的とする。

【0009】

【課題を解決するための手段】

図1は本発明の概要を説明する図である。同図において、1はサーバ、2はネットワーク接続装置である。本発明においては、ネットワーク接続装置を統合し、従来サーバ上に配置していたパケット処理部とセッション管理部をネットワーク接続装置2上に配置してパケット中継処理部を構成し、該パケット中継処理部により、ネットワーク接続装置2上でセッション管理に基づくパケット中継処理を行う。

【0010】

また、ネットワーク接続装置2上に、処理振分部2cと複数のサービス処理部2dを設け、サーバ1により設定されるポリシーに従って、処理振分部2cにより、複数のサービス処理部2dへのセッション管理に基づく振り分けを行う。

【 0 0 1 1 】

さらに、サーバ 1 に外部セッション管理機能を設け、セッション数がネットワーク接続装置 2 のセッションテーブル登録数を上回った場合等に、サーバ 1 によりセッション管理を行うようにすることもできる。

【 0 0 1 2 】

また、サーバ 1 に外部サービス処理部を設け、上記処理振分部 2 c が、パケットを上記サーバ 1 に転送し、サーバ 1 の外部サービス処理部でサービス処理を実行させるようにしたり、サーバ 1 にパケット詳細解析部を設け、サーバ 1 がパケットを解析してサービスを決定し、決定したサービス内容をネットワーク接続装置 2 に設定し、ネットワーク接続装置 2 は、以後同じセッションに対して上記決定されたサービス内容に基づき中継処理を行うようにすることもできる。

【 0 0 1 3 】

以上のように本発明においては、次のようにして前記課題を解決する。

(1) 上記ネットワーク接続装置 2 に、パケット処理部 2 a とセッション管理部 2 b からなる、セッション管理に基づくパケット中継処理部を設け、ネットワーク接続装置 2 により、セッション管理に基づく中継処理を行う。

【 0 0 1 4 】

上記のように、従来サーバ上に配置していた機能をネットワーク接続装置 2 で行っているため、サーバ 1 の CPU 使用率を下げることもできる。また、ネットワーク接続装置 2 でセッション管理を行い、セッション開始時にセッションテーブルに出力先を登録しているため、セッションの途中でルーティングテーブルが変更されても、現在継続中のセッションについては、一貫性を保持できる。

(2) 上記 (1) において、パケット中継処理装置のサーバ 1 に外部セッション管理機能を設け、ネットワーク接続装置 2 が、与えられた条件に応じてセッション情報を上記サーバ 1 に転送し、サーバ 1 によりセッション管理を行う。

【 0 0 1 5 】

これにより、セッション数がネットワーク接続装置 2 のセッションテーブル登録数を上回った場合でも、ネットワーク接続装置 2 で溢れた分をサーバ 1 で管理することができる。

(3) 上記(1)において、ネットワーク接続装置2に処理振分部2cと複数のサービス処理部2dを設け、処理振分部2cが、上記複数のサービス処理部2dへのパケットの振分を行いサービス処理を実行させる。

【0016】

上記のように、処理振分部2cと複数のサービス処理部2dをサーバ1より高速に処理できるネットワーク接続装置2に配置することにより、サーバ1のCPUの使用率を小さくすることができるとともに、サービス処理を高速化することができる。

(4) 上記(3)において、サーバ1に外部サービス処理部を設け、処理振分部2cが、与えられた条件によって、パケットの振分を行いサーバ1の外部サービス処理部でサービス処理を実行させる。

【0017】

上記のようにサービス処理を、ネットワーク接続装置2とサーバ1の両方で実行できるようにすることにより、ネットワーク接続装置2上で実現するのは困難なサービス処理をサーバ1で行うことができ、ネットワークサービスが複雑な処理を必要とする場合でも対応することができる。

(5) 上記(1)において、ネットワーク接続装置2に振分処理部2cとサービス処理部2dを設け、また、サーバ1にパケット詳細解析部(不図示)を設け、処理振分部2cが、与えられた条件によってパケットをサーバ1に転送し、サーバ1がパケットを解析してサービスを決定し、決定したサービス内容をネットワーク接続装置2に設定し、ネットワーク接続装置2は、以後同じセッションに対して上記設定されたサービス内容に基づき中継処理を行う。

【0018】

上記のように、サーバ1においてパケットを解析してサービスを決定し、決定したサービス内容をネットワーク接続装置2に設定し、以後同じセッションに対してネットワーク接続装置2が上記決定されたサービス内容に基づき中継処理を行うようにすることにより、サーバ1で全ての処理を行う場合に比べ、サービス処理を高速に実現することが可能となる。

【0019】

【発明の実施の形態】

図 2 は本発明の第 1 の実施例のネットワーク中継処理装置の構成を示す図である。

同図において、11 はサーバであり、ネットワーク制御部 12 を備えており、ネットワーク制御部 12 は、管理者が入力したルーティング情報を制御情報通信部 31 を通して、ネットワーク接続装置 20 のルーティングテーブル 23 a に書き込む。制御情報通信部 31 は、例えば P C I (Peripheral Components Interconnect) バスやシリアルインターフェースである。

【0020】

20 はネットワーク接続装置であり、本実施例のネットワーク接続装置 20 は、図 39 に示した複数のネットワーク接続装置 104 を統合したものであり、パケット処理部 21、セッション管理部 22、セッションテーブル 22 a、ルーティング処理部 23、ルーティングテーブル 23 a を備え、前記図 38 のサーバが行っていた、パケット処理、セッション管理、ルーティング処理等は、ネットワーク接続装置 20 で行われる。

【0021】

図 2 において、ネットワークから入力された図 3 に示すパケットは、ネットワーク接続部 30 を通してネットワーク接続装置 20 のパケット処理部 21 に送られる。ネットワーク接続部 30 は、例えばイーサネット（登録商標）コントローラである。

【0022】

パケット処理部 21 では、後述する図 4 のフローチャートに示す処理を行い、パケットをセッション管理部 22 に送る。セッション管理部 22 では、後述する図 5 のフローチャートに示すようにセッション管理を行い、パケットをパケット処理部 21 に渡す。

【0023】

パケット処理部 21 は、後述する図 4 に示すようにパケットの処理を行い、パケットをネットワーク接続部 30 を介して、ネットワークに出力する。

図 4 に上記パケット処理部の処理フローを示す。

【0024】

同図に示すように、パケット処理部 21 は、ネットワークから入力されたパケットのバッファリングを行い（ステップ S1）、チェックサムのチェックを行う（ステップ S2）。ついで、パケット処理部 21 は、パケットのデフラグメンテーションを行い（ステップ S3）、パケットをセッション管理部 22 へ送る（ステップ S4）。

【0025】

そして、パケット処理部 21 は、セッション管理部 22 から送られてくるパケットのフラグメンテーション（ステップ S5）、チェックサム再計算を行い（ステップ S6）、パケットをネットワークに出力する。なお、パケット処理部 21 における処理は従来のパケット処理部における処理と同じである。

【0026】

図 5 に上記セッション管理部 22 の処理フローを示す。

同図に示すように、セッション管理部 22 にパケットが送られてくると、セッション管理部 22 では、そのパケットに対応するセッションデータをセッションテーブル 22a から検索する（ステップ S11）。セッションテーブル 22a は、セッションを管理するためのセッションデータを格納するテーブルである。図 6 にセッションテーブル 22a の構成例を示す。図 6 に示すように、セッションデータは、セッションを識別するセッション ID (Identifier)、セッションを一意に決定するためのセッション検索キー（宛先／送信元アドレス、宛先／送信元ポート、プロトコル）、セッションの状態、および出力先などを項目として持つ。

【0027】

ステップ S11 において、セッション管理部 22 は、パケットの IP ヘッダ内の送信元／宛先 IP アドレス、及び TCP ヘッダ内のプロトコル、送信元／宛先ポート等の情報をキーにしてセッションテーブル 22a を検索する。

【0028】

セッション管理部 22 に送られてきたパケットのヘッダ内の情報とセッション検索キーが一致するセッションデータが、セッションテーブル 22a に登録されていない場合には（ステップ S12：No）、その送られてきたパケットは、あ

るセッションの最初の packets であるので、セッション管理部 22 は、セッションテーブル 22 a にそのセッションに関するセッションデータを登録する（ステップ S13）。すなわち、ステップ S13 において、セッション管理部 22 は、送られてきた packets のヘッダ内の情報に基づいて、図 6 に示すセッションテーブル 22 a にセッション検索キー（宛先/送信元アドレス、宛先/送信元ポート、プロトコル）や、セッションの状態を書き込む。

【0029】

ついで、ルーティング処理部 23 でルーティングテーブル 23 a の検索を行い、検索の結果として得られた出力先をセッションテーブル 22 a に書き込む（ステップ S14）。

【0030】

一方、セッションテーブル 22 a にその packets のヘッダ内の情報とセッション検索キーが一致するセッションデータが登録されている場合には（ステップ S12: Yes）、セッション管理部 22 は、そのセッションの状態を検査して、状態が遷移するかどうかを判定する（ステップ S15）。そして、状態が遷移する場合には（ステップ S15: Yes）、セッション管理部 22 は、セッションテーブル 22 a 内のセッション状態を書き換える（ステップ S16）。

【0031】

そして、セッション管理部 22 は、セッションの状態遷移が終わりセッションクローズの場合、すなわちセッション状態が TIME_WAIT 及び CLOSED になっている場合には（ステップ S17: Yes）、そのセッションに関するセッション検索キー、セッション状態および出力先等をセッションテーブル 22 a のエントリから削除する（ステップ S18）。そして、処理が終わった packets は出力先に送られる。セッションの状態がセッションクローズになっていない場合は（ステップ S17: No）、セッション管理部 22 はステップ S18 を行わず、処理が終わった packets は出力先に送られる。

【0032】

上記状態遷移は、TCP とその他のプロトコルではその判断が異なる。以下、TCP とその他のプロトコルを分けて説明する。

図7にTCPの場合のセッション状態を示す。TCPの場合、セッション状態には図7に示すように、CLOSED、SYN_RECV、ESTAB、FIN_RECV、FIN_SENT、TIME_WAITの6つの状態を設定する。

【0033】

セッションテーブル22aのセッション状態には、図6に示すようにCLOSEDを除く上記5つの状態のうち、どの状態であるかが書き込まれている。

セッションが登録されていない時には状態がCLOSEDになっており、この状態でSYNパケットが到着した場合、セッション状態はSYN_RECVに状態遷移する。その際、セッション管理部22は、セッションテーブル22aの「セッション状態」をSYN_RECVに書き換える。ついで、セッション状態は、ESTAB〈Established〉状態に遷移し、パケットが送受信される。そして、FINパケットによりセッションは終了する。以下同様にして、SYNパケットとFINパケットの到着を検知することにより、セッション管理部22は、セッションの開始と終了を検知することができる。

【0034】

図8にTCPの場合のセッション開始からセッション終了までの状態遷移の様子の一例を示す。

同図に示すように、クライアントとサーバ間で通信を行う場合、まずクライアントからSYNパケットを送信する。ついで、サーバからSYN_ACKパケットを返し、これに応答してクライアントからサーバにACKパケットを送信する。これにより、セッション状態は、SYN状態からESTAB (Established) 状態に遷移し、以後、クライアントとサーバは、相互にパケットを送受信する。そして、セッションを終了する際、例えばクライアントからFINパケットをサーバに送信し、サーバがFIN_ACKパケットをクライアントに送信し、これに応答してクライアントからACKパケットをサーバに送信することによりセッションが終了する (CLOSED状態となる)。

【0035】

これに対し、TCP以外では、パケットにSYNやFINのフラグが存在しない。図9に一例としてUDPの場合の状態遷移を示す。図9に示すようにセッシ

セッションテーブル 2 2 a に登録されていないセッションに属するパケットが届いた場合には、セッション管理部 2 2 は、そのセッションの状態を E S T A B とする。セッションの終了は検知することができないので、セッション管理部 2 2 は、タイマーによって一定時間パケットの通過が無い場合にはそのセッションをセッションテーブル 2 2 a から削除することによって対応する。

【 0 0 3 6 】

以上説明したように、本実施例においては、ネットワーク接続装置 2 0 にセッション管理に基づくパケット中継処理機能を設け、従来サーバ 1 1 上に配置していた機能をネットワーク接続装置 2 0 が果たすようにしたので、サーバ 1 1 の C P U の使用率を下げることができる。

【 0 0 3 7 】

また、ネットワーク接続装置 2 0 にセッション管理部 2 2 を設け、セッション開始時にセッションテーブル 2 2 a に出力先を登録しているので、セッションの途中でルーティングテーブル 2 3 a のエントリが変更されても、現在継続中のセッションについては、一貫性を保持できる。

【 0 0 3 8 】

図 1 0 は本発明の第 2 の実施例のパケット中継処理装置の構成を示す図である。本実施例は、前記図 2 に示した第 1 の実施例のパケット中継処理装置において、セッション情報をサーバ 1 1 に転送するサーバ転送部 2 4、セッション情報の通信を行うセッション情報通信部 3 2、外部セッション管理部 1 3、外部セッションテーブル 1 3 a を設けたものである。そして、ネットワーク接続装置 2 0 のセッションテーブル 2 2 a が一杯になったとき、サーバ 1 1 に設けた外部セッション管理部 1 3 によりセッション管理を行う。その他の動作は第 1 の実施例と同様である。

【 0 0 3 9 】

図 1 1 に本実施例におけるセッション管理部、外部セッション管理部における処理フローを示す。

同図に示すように、セッション管理部 2 2 にパケットが送られてくると、セッション管理部 2 2、外部セッション管理部 1 3 では、パケットのヘッダに格納さ

れた情報を検索キーとしてセッションテーブル22a、外部セッションテーブル13aを検索する(ステップS21)。セッションテーブル22a、13aは前記図6で説明したセッションを管理するための情報を格納したテーブルである。

【0040】

セッション管理部22に送られてきたパケットのヘッダ内の情報とセッション検索キーが一致するセッションデータがセッションテーブル22a及び外部セッションテーブル13aに登録されていない場合には(ステップS22:No)、そのパケットは、あるセッションの最初のパケットであるので、まず、セッション管理部22は、セッションテーブル22aが一杯かを調べる(ステップS23)。

【0041】

セッションテーブル22aが一杯でない場合には(ステップS23:No)、セッション管理部22は、前記したようにセッションテーブル22aにそのセッションのセッションデータの登録を行う(ステップS24)。ついで、ルーティング処理部23でルーティングテーブル23aの検索を行い、結果をセッションテーブル22aに出力先を書き込む(ステップS25)。

【0042】

また、セッションテーブル22aに、パケットのヘッダ内の情報とセッション検索キーが一致するセッションデータが登録されている場合には(ステップS22:Yes)、セッション管理部22はセッション状態を検査して、状態が遷移するかどうかを判定する(ステップS26)。そして、状態が遷移する場合には(ステップS26:Yes)、セッション管理部22は、セッションテーブル22aに格納されたセッションデータのセッション状態を書き換える(ステップS27)。

【0043】

そして、セッションの状態遷移が終わった後、セッションクローズの場合には(ステップS28:Yes)、セッション管理部22は、セッションテーブル22aのエントリからそのセッションデータを削除する(ステップS29)。処理が終わったパケットは出力先に送られる。

【0044】

一方、セッションの最初の packets を登録する際、セッションテーブル 22a が一杯の場合には（ステップ S23：Yes）、サーバ 11 の外部セッション管理部 13 で上記と同様の処理を行う。

【0045】

すなわち、前記ステップ S24 およびステップ S25 で説明したようにして、外部セッション管理部 13 は、外部セッションテーブル 13a にその packets のセッションのセッションデータを登録し（ステップ S30）、ルーティング処理部 23 は、ルーティングテーブルの検索を行って、結果を外部セッションテーブル 13a に出力先を書き込む（ステップ S31）。

【0046】

また、外部セッションテーブル 13a にその packets のヘッダ内の情報とセッション検索キーが一致するセッションデータが登録されている場合には（ステップ S22：Yes）、外部セッション管理部 13 は、外部セッションテーブル 13a のセッション状態を検査して、セッション状態が遷移するかどうかを判定する（ステップ S26）。状態が遷移する場合には、外部セッション管理部 13 は、外部セッションテーブル 13a の「セッション状態」を書き換える（ステップ S27）。そして、セッションの状態遷移が終わった後、セッションクローズの場合には（ステップ S28：Yes）、外部セッション管理部 13 は、セッションテーブル 13a のエントリからそのセッションデータを削除する（ステップ S29）。

【0047】

以上のように、本実施例においては、ネットワーク接続装置 20 にセッション管理に基づく packets 中継処理機能を設け、従来サーバ 11 上に配置していた機能をネットワーク接続装置 20 が果たすようにしたので、第 1 の実施例と同様、サーバ 11 の CPU の使用率を下げることができる。また、第 1 の実施例と同様、セッションの途中でルーティングテーブルが変更されても、現在継続中のセッションについては、一貫性を保持できる。

【0048】

さらに、セッション数がネットワーク接続装置20のセッションテーブルに登録できる数を上回った場合、サーバ11に設けた外部セッション管理部13でセッション管理を行っているので、ネットワーク接続装置20で溢れた分をサーバ11で管理することが可能となる。

【0049】

なお、上記説明ではサーバ11に外部セッション管理部13を設けてサーバ11でセッション管理を行っているが、サーバ11に外部セッションテーブル13aのみを設け、セッション管理はネットワーク接続装置20のセッション管理部22で行い、セッションテーブル22aで溢れたセッションを上記外部セッションテーブル13aに登録するようにしてもよい。

【0050】

図12は本発明の第3の実施例のパケット中継処理装置の構成を示す図である。本実施例によれば、ネットワーク接続装置20に処理振分部26とサービス処理部27とポリシーテーブル25を設け、サーバ11により設定されるポリシーに従って、ネットワーク接続装置20がフィルタリング、負荷分散、NAT等のサービス処理を実行する。

【0051】

同図において、11はサーバであり、サーバ11はサービス制御部14を備えており、サービス制御部14は、制御情報通信部31を通して、ネットワーク接続装置20のポリシーテーブル25にポリシーを書き込む。ここで、ポリシーとは、フィルタリング、負荷分散等のサービスを実行するためのルールである。例えば、フィルタリングの場合には、ポリシーに基づいて、ポリシー検索キーの範囲でパケットを廃棄するか通過させるかが設定される。負荷分散の場合には、ポリシーに基づいて、仮想（代表）IPアドレス：ポート番号と、振分先全てのサーバのIPアドレス：ポート番号が設定される。NATの場合には、ポリシーに基づいて、変換後IPアドレス：ポート番号が設定される。

【0052】

20はネットワーク接続装置であり、本実施例のネットワーク接続装置20は、第1の実施例と同様、パケット処理部21、セッション管理部22、セッシ

ンテーブル 2 2 a' を備え、さらに、上記ポリシーテーブル 2 5、処理振分部 2 6 及び複数のサービス処理部 2 7 を備える。サービス処理部 2 7 は、パケットに適用されるサービスのタイプに応じて複数備えられる。

【 0 0 5 3 】

本実施例によれば、セッション管理部 2 2 は、パケットを受信した場合、受信したパケットのヘッダ内の情報を用いて、セッションテーブル 2 2 a' からセッションデータを検索する。そして、そのパケットのヘッダ内の情報が示すセッションデータがセッションテーブル 2 2 a' に登録されている場合、上記とほぼ同様な処理が行われる。

【 0 0 5 4 】

一方、そのパケットのヘッダ内の情報によって示されるセッションデータがセッションテーブル 2 2 a' に登録されていない場合、セッション管理部 2 2 は、ポリシーテーブル 2 5 を参照し、そのパケットに適用されるべきポリシーに基づいて、セッションデータを作成し、作成したセッションデータをセッションテーブル 2 2 a' に格納する。

【 0 0 5 5 】

処理振分部 2 6 は、パケットに対する適用サービスをセッションテーブル 2 2 a' に格納されたセッションデータに基づいて判別し、判別された適用サービスに対応するサービス処理部 2 7 に処理を振り分ける。複数のサービス処理部 2 7 は、各サービスに必要な処理を行う。

【 0 0 5 6 】

以下、図 1 3 及び図 1 4 を用いて、本実施例に係わるセッションテーブル 2 2 a' 及びポリシーテーブル 2 5 について説明する。図 1 3 に、本実施例に係わるセッションテーブル 2 2 a' の構造例を示す。セッションテーブル 2 2 a' は、前記したようにセッションを管理するセッションデータを格納するテーブルである。セッションデータは、セッション ID、セッション検索キー（宛先／送信元アドレスおよびポート、プロトコル等）や、セッションの状態、および出力先等を項目として含む。本実施例においては、図 1 3 に示すように、セッションデータは、上記情報に加えて、さらに、適用サービスタイプ（フィルタリングや負荷

分散など)、そのサービス固有情報(振分先アドレスなど)、一貫性保持時間、イベントフラグ等を項目として含む。適用サービスタイプは、パケットに適用すべきサービスを示す。サービス固有情報は、適用すべきサービスに固有な情報を示す。例えば、適用サービスタイプが負荷分散である場合、サービス固有情報として振分先のアドレスが考えられる。一貫性保持時間は、セッションが終了してからセッションデータを保持すべき時間を示す。つまり、一貫性保持時間が経過するまで、セッションが終了してもセッションデータはセッションテーブル 22 a' から削除されない。イベントフラグは、そのパケットまたはパケットのヘッダのログを採取すべきか否かを示す。イベントフラグが「オン」である場合、そのパケットまたはパケットのヘッダは、サーバに転送され、サーバによってログが採取される。

【0057】

図14に、ポリシーテーブルの構成例を示す。ポリシーテーブルは、パケットに対してサービスを実行するためのルールであるポリシーを格納する。図14に示すようにポリシーは、ポリシーID、ポリシー検索キー、適用サービスタイプ、サービス固有情報、優先度、グループID、イベントフラグ、一貫性保持時間及びポリシーヒット数を含む。

【0058】

ポリシーIDは、ポリシーを識別する情報である。ポリシー検索キーは、パケットに適用すべきポリシーを決定するための情報である。適用サービスタイプは、ポリシーに基づいてパケットに適用されるサービスを示す。サービス固有情報は、セッションデータと同様に、適用サービスに固有な情報を示す。優先度は、ポリシーの優先順位を示す数値である。優先度の値が低いほど、そのポリシーは優先される。優先度は、パケットのヘッダ内の情報が、複数のポリシーのポリシー検索キーに一致した場合、どのポリシーを優先すべきか決定する際に用いられる。グループIDは、ポリシーが属するグループを識別する情報である。イベントフラグ及び一貫性保持時間は、セッションデータと同様である。ポリシーヒット数は、そのポリシーに該当したセッションのカウント値を格納する。

【0059】

イベントフラグ、一貫性保持時間、グループID及びポリシーヒット数を用いた処理についての説明は、各変形例の変形例として後述する。

以下、図12に示す第3実施例にかかわるパケット中継処理装置の動作について図15から図19を用いて説明する。

【0060】

まず、図12に示すパケット中継処理装置において、ネットワークから入力されたパケットは、ネットワーク接続部30を通り、パケット処理部21に送られる。

【0061】

パケット処理部21は、前記した図4の処理フローに示したように、入力したパケットのバッファリングとチェックサムのチェック、デフラグメンテーションを行った後、そのパケットをセッション管理部22へ送る。そして、パケット処理部21は、セッション管理部22から送られてきたパケットに対して、フラグメントとチェックサム再計算を行い、ネットワーク接続装置30を介して、ネットワークに出力する。

【0062】

本実施例のセッション管理部22の処理フローを図15に示す。

同図に示すように、パケットがセッション管理部22に送られてくると、セッション管理部22は、そのパケットのヘッダ内の情報を用いて図13に示すセッションテーブル22a'からセッションデータを検索する（ステップS41）。

【0063】

セッションテーブルの検索は、第1の実施例と同様、パケットのIPヘッダ内の送信元／宛先IPアドレス、及びTCPヘッダ内のプロトコル、送信元／宛先ポートの情報をキーにして行われる。

【0064】

パケットのヘッダ内の情報とセッション検索キーが一致するセッションデータがセッションテーブル22a'に登録されていない場合（ステップS42：No）、セッションの最初のパケットであるので、セッション管理部22は、そのセッションに対する適用サービスを判定するため、パケットのヘッダ内の情報を用

いて、図14に示すポリシーテーブル25からポリシーを検索する（ステップS43）。

【0065】

ポリシーテーブル25は、ルーティング情報を持つとともに、サービスを適用する範囲を指定するポリシー検索キー（宛先/送信元アドレスおよびポート、プロトコル。任意や範囲指定でもよい）や適用サービスタイプ（フィルタリング廃棄や負荷分散など）、そのサービス固有の情報（全ての振り分け先アドレスなど）、および、優先度を持つ。

【0066】

検索の結果、ポリシーテーブル25のエントリとパケットのヘッダ内の情報がマッチした場合、そのポリシーをセッションテーブル22a'の適用サービスタイプの欄に書き込む。つまり、セッション管理部22は、パケットのヘッダに格納された情報と適合するポリシー検索キーを持つポリシーをポリシーテーブル25から取得する。続いて、セッション管理部22は、パケットのヘッダ内の情報をセッション検索キーとするセッションデータを作成し、セッションテーブル22a'に登録する。さらに、セッション管理部22は、ポリシーに含まれる適用サービスタイプ及びサービス固有情報を、それぞれ登録したセッションデータの適用サービスタイプ欄及びサービス固有情報欄に書き込む（ステップS44）。

【0067】

ただし、複数のポリシーにマッチした場合には、ポリシーテーブル25の優先度が高い順に処理する。また、同一サービスが複数マッチした場合には、優先度が最も高いものを採用し、残りを無効とする。

【0068】

以下、ポリシーテーブル25を検索した際、パケットのヘッダに格納された情報と適合するポリシー検索キーを持つポリシーが複数存在した場合の処理について、より具体的に説明する。

【0069】

まず、取得した複数のポリシーに含まれる適用サービスタイプが互いに競合しない場合、セッション管理部22は、ポリシーの優先度の値が低い順に（つまり

、優先順位が高い順に)、複数の適用サービスタイプをセッションデータの適用サービスタイプの欄に書き込む。これにより、そのパケットは、優先順位が高い順に複数の適用サービスをうけることになる。

【 0 0 7 0 】

また、取得した複数のポリシーに含まれる適用サービスタイプが互いに競合する場合、セッション管理部 2 2 は、複数のポリシーのうち、ポリシーの優先度の値が最も低いポリシーの適用サービスタイプのみをセッションデータの適用サービスタイプの欄に書き込む。これにより、そのパケットは、最も優先順位が高い適用サービスのみを受けることとなる。

【 0 0 7 1 】

以下、具体例を挙げて説明する。あるパケットのヘッダに格納された情報と適合するポリシー検索キーを持つポリシーとして、以下の 6 ポリシーが取得されたとする。

ポリシー 1 : 適用サービス=フィルタ通過、優先度=1 0

ポリシー 2 : 適用サービス=フィルタ通過、優先度=1 0 0

ポリシー 3 : 適用サービス=フィルタ通過、優先度=2 0 0

ポリシー 4 : 適用サービス=負荷分散、優先度=1 0 0 0

ポリシー 5 : 適用サービス=負荷分散、優先度=2 0 0 0

ポリシー 6 : 適用サービス=負荷分散、優先度=3 0 0 0

この場合、フィルタ通過と負荷分散は、互いに競合しない適用サービスタイプである。また、ポリシー 1 からポリシー 3 までの適用サービスタイプは全てフィルタ通過であるため、互いに競合する。同様に、ポリシー 4 からポリシー 6 までの適用サービスタイプは全て負荷分散であるため、互いに競合する。セッション管理部 2 2 は、適用サービスタイプがフィルタ通過であるポリシーのうち、最も優先度の値が低いポリシー 1 及び、適用サービスタイプがフィルタ通過であるポリシーのうち、最も優先度の値が低いポリシー 4 を採用する。続いて、ポリシー 1 のフィルタ通過の優先度は、ポリシー 4 の負荷分散の優先度よりも低いため、セッション管理部 2 2 は、セッションデータの適用サービスタイプの欄に、フィルタ通過を先にして、フィルタ通過及び負荷分散を書き込む。これにより、その

パケットは、フィルタ通過の後に負荷分散サービスを受けることになる。

【0072】

ステップS42でYesであった場合に行われるステップS45からステップS48までのセッション状態遷移に関する処理は、第1の実施例で説明したのと同様である。すなわち、セッションテーブル22a'にセッションデータの登録がある場合には、セッション管理部22は、セッションテーブル22a'のセッション状態を検査して、状態が遷移するかどうかを判定する（ステップS45）。そして、セッションの状態が遷移する場合には（ステップS45：Yes）、セッション管理部22は、セッションテーブル22a'の状態を書き換える（ステップS46）。そして、セッションの状態遷移が終わった後、セッション管理部22は、そのセッションのセッションデータをセッションテーブル22a'のエントリから削除する（ステップS48）。処理が終わったパケットは、処理振分部26に送られる（ステップS49）。

【0073】

処理振分部26／サービス処理部27の処理フローを図16に示す。

処理振分部26／サービス処理部27では、パケットに対して適用サービスを判別し、各サービスに必要な処理を行う。

【0074】

図16において、パケットが処理振分部26に入力されると、処理振分部26は、そのパケットのヘッダ内の情報を用いてセッションテーブル22a'から、入力したパケットに対応するセッションデータを検索する。検索の結果、得られたセッションデータで示される適用サービスタイプが、ルーティング処理である場合（ステップS51）、処理振分部26は、ルーティング処理を行うサービス処理部27に処理を振り分ける。

【0075】

入力パケットに対応するセッションテーブル22a'に、ルーティング先が書き込まれていない場合、ポリシーテーブル25のルーティングテーブル（不図示）を引き、出力先インターフェースと宛先MACアドレスをセッションテーブル22a'に書き込む。

【 0 0 7 6 】

より具体的に説明すると、処理振分部 2 6 は、そのセッションデータにルーティング先が含まれているか否か判定する（ステップ S 5 1）。セッションデータにルーティング先が含まれていない場合（ステップ S 5 1 : Y e s）、処理を振り分けられたサービス処理部 2 7 は、そのセッションデータに含まれる宛先 I P アドレスを用いてルーティングテーブル（図 1 2 では不図示）を検索し、検索の結果得られた出力先インターフェースと宛先 M A C アドレスをルーティング先として決定し（ステップ S 5 2）、決定されたルーティング先をそのセッションデータに書き込む（ステップ S 5 3）。以後、そのセッションデータに対応するセッションのパケットは、決定されたルーティング先に転送される。続いて、サービス処理部 2 7 は、ステップ S 5 6 へ進む。

【 0 0 7 7 】

また、処理振分部 2 6 が、セッションテーブル 2 2 a' を検索した結果得られたセッションデータの適用サービスタイプ欄を参照し、入力パケットが、負荷分散サービスを受けるべきパケットであり、且つ セッションデータに振分先サーバが含まれていない、つまり、振分先サーバがまだ決定していないと判定した場合と判定した場合（ステップ S 5 6 : Y e s）、処理振分部 2 6 は、負荷分散処理を行うサービス処理部 2 7 に処理を振り分ける。処理を振り分けられたサービス処理部 2 7 は、振分先サーバを決定し（ステップ S 5 7）、決定された振分先のアドレスを対応するセッションテーブル 2 2 a' のサービス固有情報欄に書き込み（ステップ S 5 8）、ステップ S 6 1 に進む。

【 0 0 7 8 】

また、処理振分部 2 6 が、セッションテーブル 2 2 a' を検索した結果得られたセッションデータの適用サービスタイプ欄を参照し、入力パケットがフィルタリング廃棄サービスを受けるべきパケットであると判定したならば（ステップ S 6 1 : Y e s）、処理振分部 2 6 は、パケット廃棄処理を行うサービス処理部 2 7 に処理を振り分ける。処理を振り分けられたサービス処理部 2 7 は、そのパケットを廃棄し（ステップ S 6 2）、処理を終了する。ステップ S 6 1 の判定で N o である場合、ステップ S 6 3 に進む。

【 0 0 7 9 】

処理振分部 2 6 が、セッションテーブル 2 2 a' を検索した結果得られたセッションデータの適用サービスタイプ欄を参照し、入力パケットが、負荷分散もしくは NAT サービスを実行するパケットならば、その入力パケットはヘッダ書換を受けるべきパケットであると判定する（ステップ S 6 3 : Y e s）。処理振分部 2 6 は、ヘッダ書換処理を行うサービス処理部 2 7 に処理を振り分ける。処理を振り分けられたサービス処理部 2 7 は、そのパケットの IP ヘッダと TCP ヘッダ上の送信元／宛先 IP アドレス、送信元／宛先ポート等を、セッションテーブル 2 2 a' に格納されたセッションデータに従って書き換え、（ステップ S 6 4）処理を終了する。なお、セッションデータに複数の適用サービスが格納されている場合、格納されている順に、入力パケットに該複数の適用サービスを実行する。

【 0 0 8 0 】

以上のように、本実施例においては、第 1 の実施例と同様、サーバ 1 1 の CPU の使用率を下げることができ、また、セッションの途中でルーティングテーブルが変更されても、現在継続中のセッションについては、一貫性を保持できる。

【 0 0 8 1 】

さらに、処理振分部 2 6 と複数のサービスに対応した複数のサービス処理部 2 7 を、サーバ 1 1 より高速に処理できるネットワーク接続装置 2 0 に配置したので、サーバの CPU の使用率を小さくすることができるとともに、サービス処理を高速化することができる。

【 0 0 8 2 】

さらに、また、本実施例によれば、サービスに応じて複数のサービス処理部 2 7 をネットワーク接続装置 2 0 に備えることとしている。これにより、新たなサービスが必要になった場合、必要となったサービスに対応する新たなサービス処理部 2 7 をネットワーク接続装置 2 0 に追加することにより、容易に対応することが可能な柔軟な構成を実現する。例えば、新たに、VPN（Virtual Private Network）暗号化サービスや復号化サービスが必要になった場合、新たに、VPN 暗号化サービスを行うサービス処理部 2 7 及び復号化サービスを行うサービス

処理部 2 7 を追加することにより対応することが可能である。

【 0 0 8 3 】

以下、図 1 7 を用いて、より詳しくヘッダ書換処理について説明する。図 1 7 に、本実施例においてネットワーク接続装置 2 0 が負荷分散サービスを行う場合の packets フローを示す。なお、図 1 7 に示す packets フローは、図 1 3 に示すセッションテーブル 2 2 a' 内のセッション ID が 2 及び 3 であるセッションデータに対応している。また、矢印の方向は、パケットの送信される方向を示す。

【 0 0 8 4 】

アドレスが 10.25.1.230 であるクライアントからアドレスが 192.168.100.75 であるサーバへパケットが送信される場合、まず、矢印 A 1 に示すように、クライアントからネットワーク接続装置 2 0 へ「宛先アドレス：192.168.100.75、送信元アドレス：10.25.1.230」をヘッダに格納したパケット P 1 が送信される。ネットワーク接続装置 2 0 のセッション管理部 2 2 は、パケット P 1 に含まれる送信元アドレス 10.25.1.230 及び宛先アドレス 192.168.100.75 等をキーとして図 1 3 に示すセッションテーブル 2 2 a' を参照し、セッション ID = 3 であるセッションデータを取得する。

【 0 0 8 5 】

取得されたセッションデータ内の適用サービスタイプは「ヘッダ書換」であるため、ネットワーク接続装置 2 0 内の処理振分部 2 6 は、ヘッダ書換処理を行うサービス処理部 2 7 に処理を振り分ける。そのセッションデータ内の固有情報は「宛先アドレス：192.168.100.100」であるため、処理を振り分けられたサービス処理部 2 7 は、パケット P 1 内の宛先アドレスを「192.168.100.75」から「192.168.100.100」に書き換える。この結果、矢印 A 2 に示すように、ネットワーク接続装置 2 0 からアドレスが 192.168.100.100 である振分先サーバへ「宛先アドレス：192.168.100.100、送信元アドレス：10.25.1.230」をヘッダに格納したパケット P 2 が送信される。

【 0 0 8 6 】

逆に、アドレスが 192.168.100.100 である振分先サーバからアドレスが 10.25.1.230 であるクライアントへパケットが送信される場合、まず、矢印 A 3 に示す

ように、振分先サーバからネットワーク接続装置 2 0 へ「宛先アドレス：10.25.1.230、送信元アドレス：192.168.100.100」をヘッダに格納したパケット P 3 が送信される。ネットワーク接続装置 2 0 のセッション管理部 2 2 は、パケット P 3 に含まれる送信元アドレス及び宛先アドレスをキーとして図 1 3 に示すセッションテーブル 2 2 a' を参照し、セッション ID = 2 であるセッションデータを取得する。

【 0 0 8 7 】

取得されたセッションデータ内の適用サービスタイプ欄のエントリは「ヘッダ書換」であるため、ネットワーク接続装置 2 0 内の処理振分部 2 6 は、ヘッダ書換処理を行うサービス処理部 2 7 に処理を振り分ける。処理を振り分けられたサービス処理部 2 7 は、そのセッションデータ内の固有情報に基づいて、パケット内の送信元アドレスを「192.168.100.100」から「192.168.100.75」に書き換える。この結果、矢印 A 4 に示すように、ネットワーク接続装置 2 0 からアドレスが 10.25.1.230 であるクライアントへ「宛先アドレス：10.25.1.230、送信元アドレス：192.168.100.75」をヘッダに格納したパケット P 4 が送信される。このようにして、ネットワーク接続装置 2 0 は、パケットのヘッダを書き換える事により、パケットの宛先サーバの負荷を分散させることができる。

【 0 0 8 8 】

図 1 8 は本発明の第 4 の実施例のパケット中継処理装置の構成を示す図である。本実施例は、上記第 3 の実施例のパケット中継処理装置において、処理振分部 2 6 にサーバ転送機能を設けるとともに、サーバ 1 1 に外部サービス処理部 1 5 を設け、サービス処理を、ネットワーク接続装置 2 0 とサーバ 1 1 の両方で実行できるようにしたものである。本実施例において、サービス処理をサーバ 1 1 で実行する場合には、ポリシーテーブル 2 5 にサービスの内容だけでなく、サーバ 1 1 に転送することを設定しておく。その他の動作は第 3 の実施例と同様である。

【 0 0 8 9 】

図 1 8 に示すように、外部サービス処理部 1 5 は、第 3 実施例に係わるサービス処理部 2 7 と同様に、適用サービスタイプに応じて複数の外部サービス処理部

15をサーバ11に備えられる。従って、第3実施例におけるサービス処理部27と同様に、新たなサービスタイプが必要になった場合、新たなサービスタイプに対応する新たな外部サービス処理部15をサーバ11に追加することにより、容易に対応することが可能である。

【0090】

本実施例にかかわるセッションテーブル22a'及びポリシーテーブル25の構成は、第3実施例とほぼ同様であるため、詳しい説明は省略する。異なる点は、第4実施例によれば、サービス処理部27で行うサービスの内容に加えて、サーバ11に転送して外部サービス処理部15で行うサービスの内容をセッションテーブル22a'及びポリシーテーブル25に設定することができることである。

【0091】

以下、本実施例の処理振分部26、サービス処理部27及び外部サービス処理部15における処理の手順を図19に示す。図19において、ステップS51からステップS64までの処理は図16と同じである。例えば、入力パケットに対応するセッションテーブル22a'内のセッションデータで、適用サービスタイプが「ルーティング」が書き込まれ、且つ、ルーティング先が書き込まれていない場合、サービス処理部27は、ポリシーテーブル25のルーティングテーブルを引き、出力先インターフェースと宛先MACアドレスをセッションテーブル22a'内のセッションデータに書き込む。

【0092】

このように、セッションテーブル22a'の適用サービスタイプを参照し、適用サービスタイプにサーバ転送が設定されていない場合には、前記図16で説明したように、適用サービスタイプに応じた処理を行い、ヘッダ書換えパケットの場合、ヘッダの書換え処理を行う。

【0093】

さらに、本実施例によれば、サービスの一部をサーバ11内の外部サービス処理部15が行う。そのために、処理振分部26は、図16のステップS51からステップS64の処理に加えて、以下の手順を行う。

【 0 0 9 4 】

すなわち、処理振分部 2 6 は、セッションテーブル 2 2 a' を検索して得られたセッションデータの適用サービスタイプ欄を参照し、入力パケットが、サーバ 1 1 へ転送されるべきパケットであるか否かを判定する（ステップ S 7 1）。セッションデータの適用サービスタイプ欄に「サーバ転送：ON」及び適用サービスタイプが設定されている場合には（ステップ S 7 1：Yes）、処理振分部 2 6 は、パケットに転送用ヘッダを付す処理を行うサービス処理部 2 7 に処理を振り分ける。処理を振り分けられたサービス処理部 2 7 は、そのパケットに転送用ヘッダを付す。転送用ヘッダの内容は、例えば、適用サービスタイプ、そのパケットのセッションデータのセッション ID 及び入力インターフェースである。続いて、サービス処理部 2 7 は、パケット通信部 3 3 を介してパケットをサーバ 1 1 の外部サービス処理部 1 5 に転送する（ステップ S 7 2）。適用サービスタイプに対応する外部サービス処理部 1 5 は、受信したパケットを処理する（ステップ S 7 3）。

【 0 0 9 5 】

外部サービス処理部 1 5 の処理フローは前記した図 1 6 と同様である。例えば、セッションデータ内でルーティング先が未決定の場合、外部サービス処理部 1 5 は、ルーティング先を決定し、出力先インターフェースと宛先 MAC アドレスをセッションテーブル 2 2 a' に書き込む。

【 0 0 9 6 】

また、入力パケットが、負荷分散サービスをうけるべきパケットであり、セッションデータ内で振分先がまだ決定していない場合、外部サービス処理部 1 5 は、振分先サーバを決定し、対応するセッションテーブル 2 2 a' 内のセッションデータのサービス固有情報欄に書き込む。入力パケットがフィルタリング廃棄サービスを受けるべきパケットならば、外部サービス処理部 1 5 は、パケットを廃棄する。

【 0 0 9 7 】

そして、入力パケットが、負荷分散もしくは NAT サービスを受けるべきパケットならば、外部サービス処理部 1 5 は、そのパケットの IP ヘッダと TCP ヘ

ッダ上の送信元／宛先 I P アドレス、送信元／宛先ポート等を、セッションテーブル 2 2 a' 内のセッションデータに従って書き換える。

【 0 0 9 8 】

なお、以上では、外部サービス処理部 1 5 が、ネットワーク接続装置 2 0 におけるサービス内容と同じサービスを行う場合について説明したが、外部サービス処理部 1 5 で、例えば、暗号化、復号化、プロキシ、コンテンツ変換、プロトコル変換等のネットワーク接続装置 2 0 上で行わないサービス処理を行うようにしてもよい。

【 0 0 9 9 】

以上のように本実施例においては、ネットワーク接続装置 2 0 にセッション管理に基づくパケット中継処理機能を設け、従来サーバ上に配置していた機能をネットワーク接続装置 2 0 が果たすようにする。これにより、第 1 の実施例と同様、サーバの C P U の使用率を下げるができる。また、第 1 の実施例と同様、セッションの途中でルーティングテーブルが変更されても、現在継続中のセッションについては、一貫性を保持できる。さらに、処理振分部 2 6 にパケットをサーバへ転送する機能を設けるとともに、サーバ 1 1 に外部サービス処理部 1 5 を設け、サービス処理を、ネットワーク接続装置 2 0 とサーバ 1 1 の両方で実行できるようにしたので、ネットワーク接続装置 2 0 上で実現するのは困難なサービス処理をサーバ 1 1 で行うことができ、ネットワークサービスが複雑な処理を必要とする場合でも対応することができる。

【 0 1 0 0 】

次に、第 5 実施例について説明する。図 2 0 は本発明の第 5 の実施例のパケット中継処理装置の構成を示す図である。図 2 1 に示すように、本実施例に係わるパケット中継処理装置は、第 3 実施例に係わるパケット中継処理装置を構成するサーバ 1 1 にパケット詳細解析部 1 6 を更に備える。このように構成することにより、ネットワーク接続装置 2 0 の処理振分部 2 6 が、与えられた条件によってパケットをサーバ 1 1 に転送し、サーバ 1 1 内のパケット詳細解析部 1 6 がパケットを解析してサービスを決定し、決定したサービス内容をネットワーク接続装置 2 0 に設定する。そして、設定以後同じセッションに対して、ネットワーク接

続装置 20 は、上記決定されたサービス内容に基づき中継処理を行うようにしたものである。

【0101】

図 20 において、11 はサーバであり、サーバ 11 は前記第 3、第 4 の実施例と同様、サービス制御部 14 を備えており、サービス制御部 14 は、前記したように制御情報通信部 31 を通して、ネットワーク接続装置 20 のポリシーテーブル 25 にポリシーを書き込む。更に、サービス制御部 14 は、サーバ 11 が備える詳細解析用ポリシーテーブル（図 20 では不図示）にもポリシーを書き込む。

【0102】

また、サーバ 11 はパケット詳細解析部 16 を備えており、パケット詳細解析部 16 は、不図示のパケット詳細解析用のセッションテーブル及びポリシーテーブルに基づいて、パケットを解析してそのパケットを含むセッションに対するサービスを決定し、決定したサービス内容をネットワーク接続装置 20 のセッションテーブル 22 a' のセッションデータを設定しなおす。再設定後、ネットワーク接続装置 20 は上記サービス内容に基づき中継処理を行う。詳細解析用のセッションテーブル及びポリシーテーブルのデータ構成については後述する。

【0103】

第 3 及び第 4 実施例のサービス処理部 27 や外部サービス処理部 15 と同様に、パケット詳細解析部 16 も、適用サービスタイプに応じてサーバ 11 に複数備えられる。従って、新たなサービスタイプが必要になった場合、新たなサービスタイプに対応する新たなパケット詳細解析部 16 をサーバ 11 に追加することにより、容易に対応することが可能である。

【0104】

20 はネットワーク接続装置であり、本実施例のネットワーク接続装置 20 は、第 3 の実施例と同様、パケット処理部 21、セッション管理部 22、セッションテーブル 22 a'、ポリシーテーブル 25、処理振分部 26、サービス処理部 27 を備えており、さらに処理振分部 26 はパケットをサーバへ転送する機能を備えている。

【0105】

上記パケット処理部 2 1、セッション管理部 2 2、処理振分部 2 6、サービス処理部 2 7 の動作は前記第 3 の実施例と同様である。本実施例に係わるポリシーテーブル 2 5 のデータ構成は第 3 実施例と同様であるため、説明は省略する。本実施例にかかわるセッションテーブル 2 2 a' のデータ構成については、後述する。

【0106】

また、本実施例においては、予めサーバ 1 1 によりポリシーテーブル 2 5 の適用サービスの欄に、上記パケット詳細解析部 1 6 に転送するパケットと適用サービスの適用範囲（例えば h t t p は U R L フィルタリング適用対象のパケットである等）を設定する。処理振分部 2 6 は、前記第 4 の実施例で説明したのと同様に、ポリシーテーブル 2 5 を参照してサーバ 1 1 に転送するパケットを判断し、該当パケットのヘッダに適用サービスタイプの種類を付した後、そのパケットをパケット通信路 3 3 を介してサーバ 1 1 のパケット詳細解析部 1 6 に転送する。

【0107】

以下、図 2 1 から図 2 6 を用いて、本実施例にかかわる各テーブルのデータ構成について説明する。まず、図 2 1 から図 2 4 を用いて本実施例にかかわるセッションテーブル 2 2 a' について説明する。図 2 1 から図 2 4 に示すように、セッションテーブル 2 2 a' に格納されるセッションデータに含まれる項目は、図 1 3 に示すセッションテーブル 2 2 a' と同様である。しかし、本実施例によれば、セッションデータがセッションテーブル 2 2 a' に登録された後、パケット詳細解析部 1 6 が、パケットを解析し、解析結果に基づいてセッションテーブル 2 2 a' のセッションデータを再設定する。

【0108】

図 2 1 及び図 2 2 に、セッション管理部 2 2 が、ポリシーテーブル 2 5 に基づいてセッションデータを登録した際のセッションテーブル 2 2 a' の一例を示す。図 2 1 から図 2 2 に示すように、まだパケット詳細解析部 1 6 による解析が行われていないため、各セッションデータの適用サービスタイプの欄において、「サーバ転送：ON」となっている。従って、セッションデータに対応するセッションのパケットは、サーバ 1 1 に転送される。

【0109】

図23及び図24に、パケット詳細解析部16が、パケットの解析結果に基づいてセッションデータを再設定した後のセッションテーブル22a'の一例を示す。図23及び図24に示すように、パケット詳細解析部16による解析が行われたため、各セッションデータの適用サービスタイプの欄において、「サーバ転送：OFF」となっている。従って、以後、各セッションデータに対応するセッションのパケットは、サーバ11に転送されない事となる。

【0110】

また、パケット詳細解析部16によってセッションデータが再設定された結果、図21及び図22に示すセッションテーブル22a'と、図23及び図24に示すセッションテーブル22a'とは、さらに、以下の点が異なる。

【0111】

・図21に示すようにセッションID=0及び1であるセッションデータの適用サービスタイプの欄に「URLフィルタリング」が格納されている。一方、パケット詳細解析部16によるパケット解析の結果、パケットを通過させることが決定されたため、図23に示す同じセッションIDのセッションデータの同欄には、「フィルタリング通過」が格納されている。

【0112】

・図21に示すように、セッションID=2から5であるセッションデータの適用サービスタイプの欄に「URL負荷分散」が格納されているが、固有情報の欄に振分先サーバに関する情報は格納されていない。一方、パケット詳細解析部16によるパケット解析の結果、振分先サーバが決定されたため、図23に示すように、セッションID=3及び4であるセッションデータは削除され、セッションID=2及び5であるセッションデータの適用サービスタイプの欄に「ヘッダ書換」が格納され、固有情報の欄に振分先サーバに関する情報が格納されている。

【0113】

・図22に示すように、セッションID=6及び7であるセッションデータの適用サービスタイプの欄に「FTP (File Transfer Protocol) フィルタリング

」が格納されている。その後パケット詳細解析部16によるパケット解析の結果、そのセッションのパケットを通過させると決定されたため、図24に示すように、セッションID=6及び7である制御コネクションのためのセッションデータに加えて、新たにセッションID=8及び9であるデータコネクションのためのセッションデータが登録され、そのセッションデータの適用サービスタイプの欄に「フィルタリング通過」が格納されている。

【0114】

次に、図25及び図26を用いて、パケット詳細解析部16が備えるテーブルについて説明する。パケット詳細解析部16は、パケットを解析するために、詳細解析用セッションテーブル及び詳細解析用ポリシーテーブルを備える。

【0115】

図25に、詳細解析用セッションテーブルの構成例を示す。図25に示す詳細解析用セッションテーブルは、図21及び図22に示すセッションテーブル22a'に対応する。図25に示すように、詳細解析用セッションテーブルに格納されるセッションデータは、セッションID、セッション検索キー、セッション状態、関連セッション及び適用サービスタイプを項目として含む。関連セッション以外の項目は、セッションテーブル22a'に格納されるセッションデータと同様である。関連セッションは、パケット詳細解析部16がパケットを解析した結果、関連すると判定されたセッションのセッションIDである。詳細解析用セッションテーブル内のセッションデータは、セッションテーブル22a'に格納されるセッションデータに基づいて、詳細解析を行う際にパケット詳細解析部16によって登録され、詳細解析が終了するとパケット詳細解析部16によって削除される。

【0116】

図26に、詳細解析用ポリシーテーブルの構成例を示す。図26に示す詳細解析用ポリシーテーブルは、図14に示すポリシーテーブル25よりも詳しいポリシーを格納する。例えば、URLフィルタリングについては、URL毎にパケットを廃棄するか否かを示すURLフィルタリング用URLテーブルが詳細解析用ポリシーテーブルに備えられる。また、例えばFTPフィルタリングについては

、IPアドレス及びポート番号ごとに、パケットを通過させるべきか廃棄させるべきかを示すFTPフィルタリング用テーブルが備えられる。更にまた、例えば、URL負荷分散については、URL毎に振分先サーバの候補のIPアドレス及び振分方法を示すURL負荷分散用テーブル等が備えられる。なお、図25に示す詳細解析用セッションテーブルは、図21から図24に示すセッションテーブル22a'に対応している。

【0117】

以下、図27を用いて第5実施例に係わるパケット中継処理装置の動作概念について説明する。図27において、実線の矢印は、パケットの進む方向を示し、破線の矢印は、テーブル内のデータの読み込み及びテーブルへのデータ書き込みを示す。

【0118】

まず、サーバ11内のサービス制御部14は、制御情報通信部31を介して、ネットワーク接続装置20のポリシーテーブル25及びパケット詳細解析部16内の詳細解析用ポリシーテーブルにポリシーを書き込む（矢印A11）。

【0119】

続いて、ネットワーク接続装置20にパケットが入力されると、セッション管理部22は、パケットのヘッダに格納された情報を用いてポリシーテーブル25を参照し、ヘッダ内の情報とポリシー検索キーがマッチするポリシーを取得し、そのポリシーに基づいてセッションデータを作成し、セッションテーブル22a'に格納する（矢印A12）。

【0120】

そのセッションデータの適用サービスタイプの欄に「サーバ転送：ON」が格納されている場合、処理振分部26は、パケット通信部33を介してそのパケットをパケット詳細解析部16に転送する。パケット詳細解析部16は、詳細解析用ポリシーテーブル及び詳細解析用セッションテーブルを用いてそのパケットを解析する（矢印A13）。パケット詳細解析部16は、パケットの解析結果に基づいて、ネットワーク接続装置20内のセッションテーブル22a'に格納されたセッションデータを再設定する（矢印A14）。パケットの解析後は、ネットワ

ーク接続装置 2 0 に入力したパケットは、パケット詳細解析部 1 6 によって解析されることなく、サービス処理部 2 7 によって処理され、ネットワーク接続装置 2 0 から出力される（矢印 A 1 5）。

【 0 1 2 1 】

以下、第 5 実施例に係わるパケット中継処理装置の動作について説明する。パケット処理部 2 1 及びセッション管理部 2 2 による処理の手順は、第 1 から第 4 実施例と同様であるため、説明を省略する。以下、処理振分部 2 6、サービス処理部 2 7 及びパケット詳細解析部 1 6 による処理の手順に重点をおいて説明する。

【 0 1 2 2 】

図 2 8 は処理振分部 2 6 及びサービス処理部 2 7 の処理フローを示す図である。図 2 8 に示す処理のうち、ヘッダ書換処理（ステップ S 6 4）までの処理は図 1 9 と同じである。さらに、第 5 実施例によれば、処理振分部 2 6 は、セッションデータに含まれる適用サービスタイプに基づいて、入力パケットがサーバ 1 1 に転送すべき該当パケットであるか否かを判断する（ステップ S 8 1）。適用サービスタイプに「サーバ転送：ON」及び適用サービスタイプが設定されている場合には、振分処理部 2 6 は、そのパケットをサーバ 1 1 に転送すべきパケットであると判断し（ステップ S 8 1：Yes）、パケットに転送用ヘッダを付す処理を行うサービス処理部 2 7 に、処理を振り分ける。処理を振り分けられたサービス処理部 2 7 は、そのパケットに転送用ヘッダを付す。転送用ヘッダの内容は第 4 実施例と同様である。転送用ヘッダを付されたパケットは、パケット通信部 3 3 を介して、サーバ 1 1 のパケット詳細解析部 1 6 に転送される（ステップ S 8 2）。パケット詳細解析部 1 6 は、受信したパケットを解析し、解析結果に基づいて、制御情報通信部 3 1 を介して、セッションテーブル 2 2 a' に格納されたセッションデータを再設定する（ステップ S 8 3）。

【 0 1 2 3 】

図 2 9 は、パケット詳細解析部 1 6 の処理の手順を示すフローチャートである。図 2 9 に示す処理は、図 2 8 のステップ S 8 3 に相当する。本実施例においては、例として、URL フィルタリング、URL 負荷分散、及び FTP フィルタリ

ングサービスをパケット詳細解析部16を用いて提供する場合について説明する。

【0124】

まず、URLフィルタリングサービスについて説明する。

予めサーバ11のサービス制御部14が、「パケット詳細解析部16へパケットを転送しURLフィルタリングを行う」というポリシーを、制御通信情報部31を介してポリシーテーブル25に設定する。

【0125】

設定された条件から、ネットワーク接続装置20の処理振分部26が、該当パケットをパケット詳細解析部16に転送する。

パケット詳細解析部16では、受信したパケットの転送用ヘッダ内に含まれる適用サービスタイプ「URLフィルタリング」に基づいて、そのパケットがURLフィルタリングサービスを受けるべきパケットであることを判定する。パケット詳細解析部16は、受信したパケットに含まれる情報に基づいてセッションデータを作成し、詳細解析用セッションテーブルに格納する（ステップS91：Yes）。以後、パケット詳細解析部16は、そのセッションの状態を管理し、HTTPのGETリクエストを受信するまで、受信したパケットをそのままネットワークへ出力させる。

【0126】

セッション状態がESTABとなった後、HTTPのGETリクエストを受信した場合（ステップS92：Yes）、パケット詳細解析部16は、URLを判定し、パケットの通過／廃棄を決定する。すなわち、パケット詳細解析部16は、そのパケットに含まれるURLを用いて、予め設定された詳細解析用ポリシーテーブルに含まれるURLフィルタリング用URLテーブルを参照することにより、そのパケットの通過／廃棄を判定する（ステップS93）。

【0127】

パケットを廃棄すると判定した場合には（ステップS93：Yes）、パケット詳細解析部16は、そのセッションのパケットを廃棄する（ステップS103）。更に、パケット詳細解析部16は、パケットに含まれるセッションIDを用

いてセッションテーブル 2 2 a' を参照し、セッション ID に対応するセッションデータの適用サービスタイプの欄を、「サーバ転送：ON・URL フィルタリング」から「廃棄」に書き換える（不図示）。

【 0 1 2 8 】

また、パケットを通過させると判定した場合には（ステップ S 9 3 : N o）、パケット詳細解析部 1 6 は、セッションテーブル 2 2 a' を参照し、パケットに含まれるセッション ID に対応するセッションデータの適用サービスタイプの欄を「サーバ転送：ON・URL フィルタリング」から「フィルタリング通過」に書き換える（ステップ S 9 4）。図 2 1 及び図 2 3 に示すセッションテーブル 2 2 a' においてセッション ID = 0 及び 1 であるセッションデータは、それぞれ、URL フィルタリングの場合の、パケット解析前後のセッションデータの一例である。

【 0 1 2 9 】

セッションテーブル 2 2 a' 内のセッションデータを再設定した後、パケット詳細解析部 1 6 は、詳細解析用セッションテーブルから、そのセッション ID に対応するセッションデータを削除する（不図示）。

【 0 1 3 0 】

上記のように、パケット詳細解析部 1 6 が、ネットワーク接続装置 2 0 のセッションテーブル 2 2 a' 内のセッションデータの適用サービスタイプを、「サーバ転送：ON」から「フィルタリング通過」または「廃棄」に設定し直すと、ネットワーク接続装置 2 0 は上記通過条件に従い、以後のパケットを処理する。すなわち、ネットワーク接続装置 2 0 は、サーバ 1 1 のパケット詳細解析部 1 6 にパケットを転送することなく、パケットを通過させたり、廃棄する。

【 0 1 3 1 】

図 3 0 は、上記 URL フィルタリングの動作を説明する図である。

クライアント、サーバ間で、SYN、SYN_ACK、ACK パケットを交換する。そのセッションが ESTAB の状態に遷移するまでは、ネットワーク接続装置 2 0 から上記パケット詳細解析部 1 6 にそれらパケットが転送され、パケット詳細解析部 1 6 は、そのセッションの状態を管理する。つまり、「ネットワー

ク接続装置 20」及び「サーバ 11」で処理が行われる。

【0132】

セッションが E S T A B 状態に遷移し、HTTP の G E T リクエスト (G E T " h t t p : / / w w w . x x x . c o . j p " のように URL が付されている) を受信すると、サーバ 11 のパケット詳細解析部 16 は、詳細解析用ポリシーに含まれる URL フィルタリング用 URL テーブルを参照して上記 URL のパケットが廃棄すべきパケットであるか通過させるべきパケットであるかを判定し、判定結果に基づいてセッションテーブル 22 a' の適用サービスタイプの欄のエントリを「廃棄」または「通過」に書き換える。

【0133】

以後、ネットワーク接続装置 20 は、セッションテーブル 22 a' に設定された適用サービスタイプに応じて、そのセッションが終了するまで、パケットを廃棄または通過させる。つまり、「ネットワーク接続装置 20」で処理が行われる。

【0134】

次に、図 29 に戻って、URL 負荷分散サービスについて説明する。

URL 負荷分散において、例えば、クライアントがある代表サーバにアクセスした後に、URL に基づいて代表サーバに接続された他のサーバを振分先サーバとして決定し、その振分先サーバにセッションを振り分けることにより、負荷を複数の振分先サーバに分散させることができる。

【0135】

URL 負荷分散を行う際、まずサーバ 11 のサービス制御部 14 が、「パケット詳細解析部 16 へパケットを転送し URL 負荷分散を行う」というポリシーを、制御通信情報部 31 を介してポリシーテーブル 25 の適用サービスタイプ欄に設定する。

【0136】

設定された条件から、ネットワーク接続装置 20 の処理振分部 26 が該当パケットをサーバ 11 のパケット詳細解析部 16 に転送する。

パケット詳細解析部 16 では、受信したパケットに含まれる適用サービスタイ

「URL 負荷分散」に基づいて、そのパケットが URL 負荷分散サービスを受けるべきパケットであることを判定する。パケット詳細解析部 16 は、URL フィルタリングの場合と同様にして、受信したパケットに含まれる情報に基づいてセッションデータを作成し、詳細解析用セッションテーブルに格納する。さらに、パケット詳細解析部 16 は、パケットのヘッダに含まれる送信元アドレス、宛先アドレス及びポート番号等に基づいて代理応答を行い、相互に関連するセッションデータを登録し、セッションデータの関連セッションの欄に、関連するセッションデータのセッション ID を格納する（ステップ S95 : Yes）。

【0137】

図 25 に示す詳細解析用セッションテーブルにおいて、セッション ID = 2 から 5 であるセッションデータは、URL 負荷分散の場合のセッションデータの一例である。図 25 において、セッション ID = 2 であるセッションデータは、セッション ID = 4 であるセッションデータと相互に関連し、セッション ID = 3 であるセッションデータは、セッション ID = 5 であるセッションデータと相互に関連している事がわかる。

【0138】

パケット詳細解析部 16 では、クライアントとサーバ 11 の間にコネクションを確立し、以後、セッションの状態を管理する。また、パケット詳細解析部 16 は、TCP (Transmission Control Protocol) を終端する機能を有し、振分先サーバが決定するまで、パケット詳細解析部 16 は、振分先サーバの変わりにクライアントに対する応答を行う。パケット詳細解析部 16 は、セッションの状態が ESTAB となった後、HTTP の GET リクエストを受信した場合（ステップ S96 : Yes）、パケット詳細解析部 16 は、パケットに含まれる URL を用いて、予め設定された詳細解析用ポリシーテーブルに含まれる URL 負荷分散用テーブルを参照して、振分先サーバを決定する（ステップ S97）。その後、サーバ 11 は、SYN、SYN_ACK、ACK パケットを交換することにより、振分先サーバとコネクションを確立する。

【0139】

さらに、パケット詳細解析部 16 は、ネットワーク接続装置 20 のセッション

データ22a'を参照し、パケットに含まれるセッションIDに対応するセッションデータを取得する。そして、パケット詳細解析部16は、取得したセッションデータに含まれる適用サービスタイプを「サーバ転送：ON・URL負荷分散」から「サーバ転送：OFF・ヘッダ書換」に書き換える。さらに、パケット詳細解析部16は、セッションデータの固有情報の欄に、決定された振分先サーバのIPアドレス等に従って、IPアドレス：ポート番号、およびシーケンス番号／ACK番号差分を設定する（ステップS98）。これにより、相互に関連していると判定された2つのセッションデータを1つのセッションデータにまとめることになるため、2つのコネクションを1つのコネクションとして扱うことが可能となる。さらに、パケット詳細解析部16は、4つのセッションデータのうち、不要になった残りの2つのデータを、セッションテーブル22a'から削除する。

【0140】

セッションテーブル22a'内のセッションデータを再設定した後、パケット詳細解析部16は、詳細解析用セッションテーブルから、そのセッションIDに対応するセッションデータを削除する（不図示）。そして、サーバ11は、振分先サーバにHTTPのGETリクエストを送出する。

【0141】

図21及び図23に示すセッションテーブル22a'内のセッションID=2から5であるセッションデータは、それぞれ、URL負荷分散の場合のパケット解析前後のセッションデータの一例である。図21におけるセッションID=2及び4である2つのセッションデータによって示される2つのコネクションは、図23において、セッションID=2であるセッションデータで示される1つのコネクションにまとめられている。同様に、図21におけるセッションID=3及び5である2つのセッションデータによって示される2つのコネクションは、図23において、セッションID=5であるセッションデータで示される1つのコネクションにまとめられている。

【0142】

パケットの解析後、パケットは、パケット詳細解析部16に送られない。ネッ

トワーク接続装置20のヘッダ書換処理を行うサービス処理部27は、セッションテーブル22a'に格納されたセッションデータ内の固有情報に基づいて、パケット内のIPアドレス：ポート番号、シーケンス番号、ACK番号を書き換えた後、そのパケットをネットワークに出力させる。

【0143】

図31は、上記URL負荷分散サービスの動作を説明する図である。

図31に示すように、クライアントとパケット中継処理装置の間でSYN、SYN_ACK、ACKパケットを交換する。セッションがESTAB状態に移り、HTTPのGETリクエストを受信すると、パケット詳細解析部16は、GETリクエストのURLを判定し、振分先サーバを決定する。

【0144】

ついで、上記と同様に、パケット中継処理装置と振分先サーバの間でSYN、SYN_ACK、ACKパケットを交換し、振分先サーバにHTTPのGETリクエストを送出する。ここまでは、「ネットワーク接続装置20」+「サーバ11」で処理が行われる。

【0145】

パケット中継処理装置から振分先サーバにHTTPのGETリクエストを送出した後、セッションが終了するまで、ネットワーク接続装置20が、セッションテーブル22a'に格納されたセッションデータに基づいて、クライアントと振分先サーバとの間の中継処理を行う。

【0146】

次に、図29に戻って、FTPフィルタリングサービスについて説明する。FTPは、制御用の制御コネクションと、1以上のデータ転送用のデータコネクションとの複数のTCPコネクションからなる。

【0147】

予めサーバ11のサービス制御部14が、「パケット詳細解析部16へパケットを転送しFTPフィルタリングを行う」というポリシーを、制御通信情報部を介してポリシーテーブル25に設定する。

【0148】

設定された条件から、ネットワーク接続装置20の処理振分部26が該当パケットを詳細解析部16に転送する。URLフィルタリングの場合と同様に、パケット詳細解析部16は、受信したパケットに含まれる適用サービスタイプに基づいて、そのパケットがFTPフィルタリングサービスを受けるべきパケットであることを判定し、パケット詳細解析部16は、詳細解析用セッションテーブルにセッションデータを格納する（ステップS99：Yes）。続いて、パケット詳細解析部16は、セッション状態を管理し、受信パケットをそのままネットワークへ出力させる。

【0149】

セッション状態がESTABとなった後、図32に示すように、FTPのPORT命令もしくは、PASV命令のACKパケットを受信すると（ステップS100：Yes）、パケット詳細解析部16は、そのパケットに含まれるIPアドレスとポート番号を判定し、判定結果に基づいて、そのセッションのパケットを通過するか廃棄するかを決定する（ステップS101）。

【0150】

すなわち、パケット詳細解析部16は、IPアドレスとポート番号を用いて予め設定された詳細解析用ポリシーテーブル内のFTPフィルタリング用テーブルを参照して、そのセッションのパケットを通過させるか廃棄するかを決定する。パケットを廃棄すると決定した場合には（ステップS101：Yes）、パケット詳細解析部16は、セッションテーブル22a'からパケットの転送用ヘッダに含まれるセッションIDに対応するセッションデータを取得し、そのセッションデータの適用サービスタイプの欄に「廃棄」を設定し、そのパケットを廃棄する（ステップS103）。

【0151】

また、そのパケットを通過させると決定した場合には（ステップS101：No）、パケット詳細解析部16は、先のPORT命令もしくはPASV命令のACKパケットのデータ部分に記述されているIPアドレスとポート番号に基づいて、データコネクションについてのセッションデータをセッションテーブル22a'に登録し、そのセッションデータの適用サービスタイプの欄に「フィルタリ

ング通過」を設定する（ステップS102）。

【0152】

上記のようにパケット詳細解析部16が、セッションテーブル22a'内のセッションデータを再設定すると、ネットワーク接続装置20は上記通過条件に従い、以後のデータコネクションに関するパケットを処理する。すなわち、サーバ11のパケット詳細解析部16にパケットを転送することなく、パケットを通過させたり、廃棄させたりする。

【0153】

図32は、上記FTPフィルタリングの動作を説明する図である。クライアント、サーバ11間で、SYN、SYN_ACK、ACKパケットを交換し、ESTABの状態に遷移するまでは、上記パケット詳細解析部16にパケットが転送され、「ネットワーク接続装置20」+「サーバ11」で処理が行われる。

【0154】

セッションの状態がESTAB状態に遷移し、FTPのPORT命令またはPASV命令のACK（IPアドレスとポート番号が付されている）を受信すると、パケット詳細解析部16は、パケットに含まれるIPアドレスとポート番号を用いて詳細解析用ポリシーテーブルを参照し、そのパケットを廃棄すべきか、通過させるべきかを決定する。そのパケットを廃棄すると決定する場合には、パケット詳細解析部16は、セッションテーブル22a'のセッションデータにパケットを廃棄する旨を設定する。そのパケットを通過させると決定する場合には、パケット詳細解析部16は、セッションテーブル22a'にデータコネクションについてのセッションデータを登録し、適用サービスタイプ欄に「通過」を設定し直す。以後、ネットワーク接続装置20は、パケットの廃棄処理又はデータコネクションのパケットの通過処理を行う。

【0155】

最後に、パケット中継処理装置がクライアントから制御コネクションのFINパケットを受信すると、ネットワーク接続装置20からパケット通信部33を介して、サーバ11のセッション詳細解析部16にそのパケットが転送される。サーバ11は、セッション詳細解析部16を介してそのセッションのクローズ処理

を行う。さらに、セッション詳細解析部 1 6 は、パケットの転送用ヘッダに含まれるセッション ID に基づいて、クローズされるセッションに関するセッションデータを削除する。

【 0 1 5 6 】

以下、図 3 3 及び図 3 4 を用いて、第 5 実施例におけるパケットのフローについて、URL 負荷分散サービスの場合を例にとって説明する。なお、各図は、図 2 1、図 2 3、図 2 5 に示すセッションテーブルに格納されたセッション ID = 2 から 5 のセッションデータに対応する。図 3 3 に、パケット詳細解析部 1 6 によってセッションデータが再設定される前のパケットフローを示す。

【 0 1 5 7 】

セッションデータが再設定される前において、矢印 A 2 1 に示すように、アドレス：ポート番号が 192.168.30.30:11950 であるクライアントからネットワーク接続装置 2 0 へ「宛先アドレス：ポート番号=192.168.200.1:http、送信元アドレス：ポート番号=192.168.30.30:11950」をヘッダに格納したパケット P 1 1 が送信される。ネットワーク接続装置 2 0 のセッション管理部 2 2 は、ポリシーテーブル 2 5 を参照し、ヘッダ内の情報とポリシー検索キーがマッチするポリシーを取得し、そのポリシーに基づいてセッション ID = 2 であるセッションデータを作成し、セッションテーブル 2 2 a' に格納する。

【 0 1 5 8 】

セッションデータ内の適用サービスタイプは「サーバ転送：ON・URL 負荷分散」であるため、ネットワーク接続装置 2 0 内の処理振分部 2 6 は、サーバ転送処理を行うサービス処理部 2 7 に処理を振り分ける。処理を振り分けられたサービス処理部 2 7 がそのパケットに転送用ヘッダを付したのち、矢印 A 2 2 に示すようにパケットはサーバ 1 1 に転送される。サーバ 1 1 のパケット詳細解析部 1 6 は、転送されたパケットに含まれる情報に基づいて、詳細解析用セッションテーブルにセッションデータを登録する。

【 0 1 5 9 】

同様に、サーバ 1 1 からクライアントへ矢印 A 2 3 から A 2 8 に示すような経路を経てパケット P 1 2、P 1 3 及び P 1 4 が出力される際に、それぞれ、

セッションID=3、4及び5であるセッションデータが、セッションテーブル22a'にセッション管理部22によって格納され、対応するセッションデータが、詳細解析用セッションテーブルにパケット詳細解析部16によって格納される。

【0160】

セッションデータを各セッションテーブルに登録した後、HTTPのGETリクエストを受信するまで、パケット詳細解析部16は、各セッションの状態を管理し、図33に示すパケットフローに基づいて、受信したパケットをネットワークへ出力する。

【0161】

その後、セッション状態がESTABとなった後、HTTPのGETリクエストを受信すると、パケット詳細解析部16は、パケットを解析し、解析結果に基づいて、セッションテーブル22a'に格納されたセッションデータを設定しなおす。再設定後のセッションデータは、図23に示す通りである。

【0162】

図34に、パケット詳細解析部16によってセッションデータが再設定された後のパケットフローを示す。セッションデータが再設定された後において、矢印A31に示すように、振分先サーバからネットワーク接続装置20へ「宛先アドレス：ポート番号として192.168.200.1:3333、送信元アドレス：ポート番号として192.168.200.10:8080」をヘッダに格納したパケットP14が送信されると、ネットワーク接続装置20の処理振分部26は、パケットのヘッダに含まれる情報を用いて、セッションテーブル22a'を参照し、セッションID=5であるセッションデータを取得し、セッションデータに基づいて、ヘッダ書換処理を行うサービス処理部27に処理を振り分ける。サービス処理部27は、そのセッションデータに基づいて、そのパケットのヘッダ内の宛先アドレス及びポート番号を「192.168.30.30:11950」に、クライアントのアドレス及びポート番号を「192.168.200.1:http」に書き換えることにより、パケットP12を作成する。その後、矢印A32に示すように、ネットワーク接続装置20は、パケットP12を振分先サーバへそのパケットを出力する。

【 0 1 6 3 】

同様に、矢印 A 3 3 に示すように、アドレス：ポート番号が 192.168.30.30:11950 であるクライアントからネットワーク接続装置 2 0 へ「宛先アドレス：ポート番号=192.168.200.1:http、送信元アドレス：ポート番号=192.168.30.30:11950」をヘッダに格納したパケット P 1 1 が送信される。ネットワーク接続装置 2 0 の処理振分部 2 6 は、パケットのヘッダに含まれる情報を用いて、セッションテーブル 2 2 a' を参照し、セッション I D = 2 であるセッションデータを取得する。この例の場合、取得したセッションデータの適用サービスタイプの欄に「サーバ転送：O F F / ヘッダ書換」が格納されているため、処理振分部 2 6 は、ヘッダ書換処理を行うサービス処理部 2 7 に処理を振り分ける。サービス処理部 2 7 は、そのセッションデータに基づいて、そのパケットのヘッダ内の宛先アドレス及びポート番号を振分先サーバのアドレス及びポート番号を「192.168.200.10:8080」に書き換えることにより、パケット P 1 3 を作成する。その後、ネットワーク接続装置 2 0 は、矢印 A 3 4 に示すように、パケット P 1 3 を振分先サーバへそのパケットを出力する。

【 0 1 6 4 】

このように、セッション詳細解析部 1 6 がパケットの解析結果に基づいてセッションデータを書き換えた後は、サーバ 1 1 を介さずに、ネットワーク接続装置 2 0 によってパケットの中継処理が行われる。

【 0 1 6 5 】

以上のように、本実施例においては、ネットワーク接続装置 2 0 にセッション管理に基づくパケット中継処理機能を設け、従来サーバ上に配置していた機能をネットワーク接続装置 2 0 が果たすようにしたので、第 1 の実施例と同様、サーバ 1 1 の C P U の使用率を下げるができる。また、第 1 の実施例と同様、セッションの途中でルーティングテーブルが変更されても、現在継続中のセッションについては、一貫性を保持できる。

【 0 1 6 6 】

さらに、第 5 実施例によれば、サーバ 1 1 のパケット詳細解析部 1 6 においてパケットを解析してサービスを決定し、決定したサービス内容をネットワーク接

続装置 2 0 に設定し、以後同じセッションに対してネットワーク接続装置 2 0 が上記決定されたサービス内容に基づき中継処理を行うようにする。従って、サーバ 1 1 で全ての処理を行う場合に比べ、サービス処理を高速に実現することができる。

【 0 1 6 7 】

以下、各実施例の変形例について説明する。まず、第 1 の変形例について説明する。第 1 実施例から第 5 実施例において、第 1 の変形例を適用することにより、セッションが終了した後すぐにセッションデータを削除するのではなく、一定時間経過した後にセッションデータをセッションテーブル 2 2 a' することとしてもよい。

【 0 1 6 8 】

そのために、第 1 の変形例によれば、図 1 3 及び図 1 4、図 2 1 から図 2 4 に示すように、ポリシーテーブル 2 5 及びセッションテーブル 2 2 a' のエントリに、さらに一貫性保持時間を含む。以下、第 1 の変形例に係わるパケット中継処理装置が行う処理について説明する。第 1 の変形例では、セッション管理部 2 2 が行う処理の一部が第 1 から第 5 実施例と異なる。第 1 の変形例を適用した場合のセッション管理部 2 2 が行う処理について、図 5 を用いて説明する。

【 0 1 6 9 】

図 5 のステップ S 1 7 において、セッション管理部 2 2 が、あるセッションがクローズしたと判定した場合（ステップ S 1 7 : Y e s）、セッション管理部 2 2 はタイマーを設定する。セッション管理部 2 2 は、セッションデータに含まれる一貫性保持時間だけ待機した後に、図 5 のステップ S 1 8 に進み、そのセッションデータをセッションテーブル 2 2 a' から削除する。

【 0 1 7 0 】

これにより、セッションが終了した後で、一貫性保持時間が経過するまでの間に、そのセッションが再度確立された場合、セッション検索キーに変更がなければ、セッション管理部 2 2 は、そのセッションを先に終了したセッションと同じセッションとして扱う事ができるようになる。例えば、負荷分散サービスにおいて、一度終了したセッションと再度確立されたセッションとで同じ振分先サーバ

にパケットを振り分けることが可能となる。延いては、セッション管理部 2 2 によるポリシーテーブル 2 5 の検索や処理振分部 2 6 によるパケットのサーバ 1 1 への転送を省略する事ができるため、高速にパケットを処理することが可能となる。

【 0 1 7 1 】

次に、第 2 の変形例について説明する。第 3 実施例から第 5 実施例において、第 2 の変形例を適用することにより、セッションに適用するポリシーの切り換えが容易にできるようにすることとしてもよい。そのために、第 2 の変形例によれば、複数のポリシーをいくつかのグループに分ける。さらに、図 1 4 に示すように、ポリシーテーブル 2 5 に格納されるポリシーは更に項目として、そのポリシーが属するグループを識別するグループ ID を含み、ネットワーク接続装置 2 0 は、更に図 3 5 に示すフラグテーブルを備える。

【 0 1 7 2 】

以下、図 3 5 を用いて、フラグテーブルのデータ構造について説明する。図 3 5 に示すように、フラグテーブルは、グループ ID に対応して、ポリシーの有効・無効を示すフラグを格納する。図 3 5 において、例として、フラグが「オフ（0）」である場合にポリシーは無効であり、フラグが「オン（1）」である場合にポリシーは有効である。

【 0 1 7 3 】

以下、第 2 の変形例に係わるパケット中継処理装置が行う処理について説明する。第 2 の変形例では、セッション管理部 2 2 が行う処理の一部が第 3 から第 5 実施例と異なる。例として、第 3 実施例に係わるセッション管理部 2 2 が行う処理を示す図 1 5 を参照しながら、第 2 の変形例を各実施例に適用することにより、セッション管理部 2 2 が行う処理が変化する点について詳しく説明する。

【 0 1 7 4 】

第 2 の変形例において、セッション管理部 2 2 は、図 1 5 のステップ S 4 3 からステップ S 4 4 の間でさらに、以下の処理を行う。まず、ステップ S 4 3 で、セッション管理部 2 2 は、ポリシーテーブル 2 5 を検索し、パケットのヘッダに格納された情報と適合するポリシー検索キーを持つポリシーを取得する。セッシ

セッション管理部 2 2 は、得られたポリシーに含まれるグループ ID を用いてフラグテーブルを参照し、そのグループ ID に対応するフラグがオンであるかオフであるか判定する。

【 0 1 7 5 】

判定の結果、フラグがオフである場合、セッション管理部 2 2 はそのポリシーを採用しない。一方、フラグがオンである場合、セッション管理部 2 2 は、そのポリシーを採用する。セッション管理部 2 2 は、ステップ S 4 4 で、そのポリシーに基づいてセッションデータを作成し、セッションテーブル 2 2 a' に格納する。これにより、採用すべきポリシーをグループ毎に切り換えることができるようになる。

【 0 1 7 6 】

例えば、複数の通常用のポリシーと複数の非常用のポリシーとを作成した場合、第 2 の変形例によれば、予め通常用のポリシーからなる通常用グループと、非常用のポリシーからなる非常用グループを定義し、ポリシーテーブル 2 5 には、通常用のポリシーも非常用のポリシーも両方登録する。また、フラグテーブルにパケット中継処理装置のユーザが有効にしておきたいグループ、つまり、通常用と非常用いずれかのグループに対応するフラグをオンにする。これにより、通常用のポリシーと非常用のポリシーを、グループ毎に容易に切り換える事が可能となる。

【 0 1 7 7 】

次に、第 3 の変形例について説明する。第 3 実施例から第 5 実施例において、第 3 の変形例を適用することにより、パケットのログを採取できるようにすることとしてもよい。そのために、第 3 の変形例によれば、図 1 3 及び図 1 4 並びに図 2 1 から図 2 4 に示すポリシーテーブル 2 5 及びセッションテーブル 2 2 a' に格納されるセッションデータ及びポリシーは、更に項目としてイベントフラグを含む。

【 0 1 7 8 】

イベントフラグには、パケットに関するイベントフラグと、ヘッダに関するイベントフラグとがある。パケットに関するイベントフラグが「オン (1) 」であ

る場合、ログ（履歴）を採取するために、そのパケットがサーバ11に転送される。ヘッダに関するイベントフラグがオンである場合、ログを採取するために、そのパケットのヘッダがサーバ11に転送される。サーバ11は、転送されたパケット又はパケットのヘッダを解析し、ログを採取する。これにより、例えば、システムに障害が生じたときに、ネットワーク管理ソフトを用いて、採取したログを解析する事により、障害から復旧するために役に立つ情報を得ることが可能となる。

【0179】

次に、第4の変形例について説明する。第4の変形例によれば、第1実施例から第5実施例に係わるネットワーク接続装置20は、パケットに関する統計情報を取得するために、更にカウンタ（不図示）を備える。上記サーバ11のネットワーク制御部12又はサービス制御部14は、カウンタの値を参照する。統計情報として、例えば、インターフェースごとのパケット入力数と出力数が考えられる。この統計情報は、クライアント等に課金を行う際等において使用することができる。

【0180】

また、第3実施例から第5実施例に対しては、更に、統計情報として、ポリシーテーブル25に格納されたポリシー毎に、そのポリシーが適用されたセッションの数、つまり、ポリシーがヒットした回数であるポリシーヒット数を得る事としても良い。

【0181】

そのために、第4の変形例によれば、図1.4に示すように、ポリシーテーブル25に格納されるポリシーは、更に項目としてポリシーヒット数を含む。そして、セッション管理部22が、新たなセッションに関するセッションデータをセッションテーブル22a'に登録するために、ポリシーテーブル25を参照して適用すべきポリシーを取得すると、カウンタは、取得されたポリシーのポリシーヒット数をインクリメントする。これにより、ネットワーク管理者は、ポリシーが有効に利用されているか否かを判断するための情報を得る事が可能となる。

【0182】

また、第3実施例から第5実施例に対しては、更に、統計情報として、負荷分散サービスにおける振分先サーバ毎に、セッションが振り分けられた回数を示す振分先ヒット数を得る事としても良い。

【0183】

そのために、図14に示すポリシーテーブル25又は、図26に示す詳細解析用ポリシーテーブルに格納された負荷分散サービスにかかわるポリシーは、更に項目として、振分先サーバアドレスごとの振分先ヒット数を含む。そして、サービス処理部27又はパケット詳細解析部16が、セッションの振分先サーバを決定する処理を行うごとに、カウンタは、振分先サーバとして決定されたサーバに対応する振分先ヒット数をインクリメントする。これにより、ネットワーク管理者は、負荷分散の振分方式が有効に動作しているか否かを判断するための情報を得ることが可能となる。

【0184】

本実施形態において説明したネットワーク接続装置20を構成する各部及びサーバ11を構成する各部が行う処理を示すプログラムは、それぞれRAM (Random Access Memory) やROM (Read Only Memory) 等のメモリに記録され、パケット中継処理装置にハードウェア或いはソフトウェアとして備えられても良い。以下、この場合について説明する。

【0185】

図36にコンピュータ（情報処理装置）の構成を示す。図36に示すように、コンピュータ40は、少なくともCPU41、メモリ42を備える。さらに、コンピュータ40は、入力装置43、出力装置44、外部記憶装置45、媒体駆動装置46、及びネットワークインターフェース47を備えることとしても良い。各装置はバス48により互いに接続されている。

【0186】

メモリ42は、例えば、ROM、RAM等を含み、処理に用いられるプログラムとデータを格納する。CPU41は、メモリ42を利用してプログラムを実行することにより、必要な処理を行う。

【0187】

2以上のコンピュータ40に、パケット中継処理装置を構成するサーバ11及びネットワーク接続装置20に相当する機能を実現させる場合、まず、図2、10、12、18、20に示すパケット中継処理装置を構成する各部によって行われる処理を示すプログラムを用意する。そして、サーバ11に備えられる各部によって行われる処理を示すプログラム（以下、サーバ11用のプログラムという）をサーバ11を実現すべきコンピュータ内のメモリ42の特定のプログラムコードセグメントに格納する。

【0188】

また、ネットワーク接続装置20に備えられる各部によって行われる処理を示すプログラム（以下、ネットワーク接続装置20用のプログラムという）を、ネットワーク接続装置20を実現すべきコンピュータ内のメモリ42の特定のプログラムコードセグメントに格納する。ここで、ネットワーク接続装置20を実現すべきコンピュータのCPUは、例えば、ネットワークプロセッサである。なお、上述の各部によって行われる処理は、上記において、各フローチャートを用いて説明されている。

【0189】

入力装置43は、例えば、キーボード、ポインティングデバイス、タッチパネル等であり、ユーザからの指示や情報の入力に用いられる。出力装置44は、例えば、ディスプレイやプリンタ等であり、コンピュータ40の利用者への問い合わせ、処理結果等の出力に用いられる。

【0190】

外部記憶装置45は、例えば、磁気ディスク装置、光ディスク装置、光磁気ディスク装置等である。この外部記憶装置45に上述のプログラムとデータを保存しておき、必要に応じて、それらをメモリ42にロードして使用することもできる。

【0191】

媒体駆動装置46は、可搬記録媒体49を駆動し、その記録内容にアクセスする。可搬記録媒体49としては、メモリカード、メモリスティック、フレキシブルディスク、CD-ROM (Compact Disc Read Only Memory)、光ディスク、

光磁気ディスク、DVD (Digital Versatile Disk) 等、任意のコンピュータで読み取り可能な記録媒体が用いられる。この可搬記録媒体49に上述のプログラムとデータを格納しておき、必要に応じて、それらをメモリ42にロードして使用することもできる。

【0192】

ネットワークインターフェース47は、LAN、WAN等の任意のネットワーク（回線）を介して外部の装置を通信し、通信に伴うデータ変換を行う。また、必要に応じて、上述のプログラムとデータを外部の装置から受け取り、それらをメモリ42にロードして使用することもできる。

【0193】

図37は、図36のコンピュータにプログラムとデータを供給することができる、コンピュータで読み取り可能な記録媒体及び伝送信号を説明する図である。

記録媒体を用いて、上述のプログラムや各テーブルに格納されるデータを、サーバ11を実現すべきコンピュータ及びネットワーク接続装置20を実現すべきコンピュータに供給することにより、2以上のコンピュータにパケット中継処理装置に相当する機能を行なわせることも可能である。

【0194】

そのためには、上述のプログラムやデータを、コンピュータで読み取り可能な記録媒体49に予め記憶させておく。そして、図37に示すように、媒体駆動装置46を用いて、記録媒体49からサーバ11用のプログラム等をサーバ11を実現すべきコンピュータに読み出させて、そのコンピュータ（サーバ11）のメモリ42や外部記憶装置45に一旦格納させ、そのコンピュータ（サーバ11）の有するCPU41にこの格納されたプログラムを読み出させて実行させる。

【0195】

同様に、記録媒体49からネットワーク接続装置20用のプログラム等をネットワーク接続装置20を実現すべきコンピュータのメモリ42等に一旦格納させ、そのコンピュータ（ネットワーク接続装置20）の有するCPU41に格納されたプログラムを読み出させて実行させる。

【0196】

また、記録媒体49からプログラム等を、サーバ11を実現すべきコンピュータ及びネットワーク接続装置20を実現すべきコンピュータに読み出させる代わりに、プログラム（データ）提供者が有するDB50から、通信回線（ネットワーク）51を介して、プログラムをそれぞれのコンピュータにダウンロードすることとしてもよい。この場合、例えば、DB50を有しプログラムを送信するコンピュータでは、上記プログラムを表現するプログラム・データをプログラム・データ・シグナルに変換し、変換されたプログラム・データ・シグナルをモデムを用いて変調することにより伝送信号を得て、得られた伝送信号を通信回線51（伝送媒体）に出力する。プログラムを受信するコンピュータでは、受信した伝送信号をモデムを用いて復調することにより、プログラム・データ・シグナルを得て、得られたプログラム・データ・シグナルを変換することにより、プログラム・データを得る。

【0197】

次に、図38を用いて、サーバ11を実現すべきコンピュータ及びネットワーク接続装置20を実現すべきコンピュータへのプログラムやデータのローディングについて、例を挙げてより詳しく説明する。

【0198】

図38に示すように、サーバ11及びネットワーク接続装置20を実現すべきコンピュータは、各々CPU及びメモリを備え、上述の制御情報通信部31を介して接続されている。また、例えば、制御情報通信部31がPCIバスである場合、ネットワーク接続装置20をPCI用のNIC（Network Interface Card）として実現しても良い。

【0199】

例えば、サーバ11用のプログラム等及びネットワーク接続装置20用のプログラム等（ファームウェア）を記録した記録媒体がある場合、まず、サーバ11を実現すべきコンピュータに備えられた不図示の媒体駆動装置を用いて記録媒体からサーバ11用のプログラム等及びネットワーク接続装置20用のプログラム等をサーバ11のメモリにロードする（矢印A41）。続いて、サーバ11のメモリに格納されたネットワーク接続装置20用のプログラム等を、制御情報通信

部 3 1 を介してネットワーク接続装置 2 0 のメモリにロードする（矢印 4 2）。
 このようにして、サーバ 1 1 を実現すべきコンピュータ及びネットワーク接続装置 2 0 を実現すべきコンピュータに、それぞれに必要なプログラム等を供給することができる。サーバ 1 1 の CPU は、サーバ 1 1 のメモリにロードされたサーバ 1 1 用のプログラムを実行し、ネットワーク接続装置 2 0 の CPU は、ネットワーク接続装置 2 0 のメモリにロードされたネットワーク接続装置 2 0 用のプログラムを実行する。

【 0 2 0 0 】

また、上述のようにプログラム等を記録媒体からロードする代わりに、予め ROM 等に記録しておくこととしても良い事は言うまでもない。また、記録媒体のかわりに伝送信号を用いてプログラム等をサーバ 1 1 を実現すべきコンピュータに供給する事としても良い。

【 0 2 0 1 】

また、ネットワーク接続装置 2 0 において、CPU の代わりに ASIC (Application Specific Integrated Circuit) を用いて、ネットワーク接続装置 2 0 を構成する各部をハードウェアで構成する事としても良い。

【 0 2 0 2 】

以上、本発明の実施形態について説明したが、本発明は上述した実施形態に限定されるものではなく、他の様々な変更が可能である。

（付記 1） ネットワーク接続装置を有するパケット中継処理装置であって、
 上記ネットワーク接続装置がセッションを管理するセッション管理部と、
 上記セッション管理部によるセッション管理に基づいてパケットを中継するパケット処理部を備えている
 ことを特徴とするパケット中継処理装置。

（付記 2） 上記ネットワーク接続装置は、更に、上記パケットのルーティング先に関するルーティング情報を格納するルーティングテーブルと、

上記セッションの開始時に、上記ルーティング情報に基づいて上記パケットのルーティング先を決定するルーティング処理部を更に備え、

上記パケット処理部は、上記パケットを上記ルーティング先に出力する、

ことを特徴とする付記 1 に記載のパケット中継処理装置。

(付記 3) 上記パケット中継処理装置は、更に、サーバを備え、

上記サーバは、上記ルーティングテーブルに上記ルーティング情報を書き込むネットワーク制御部を備える、

ことを特徴とする付記 1 に記載のパケット中継処理装置。

(付記 4) 上記パケット中継処理装置は、さらに、サーバを備え、

上記サーバは、上記セッションを管理する外部セッション管理部を備え、

上記セッション管理部は、与えられた条件に応じて上記セッションに関するセッション情報を上記サーバに転送し、

上記外部セッション管理部は、受信した上記セッション情報に基づいて上記セッションを管理する、

ことを特徴とする付記 1 に記載のパケット中継処理装置。

(付記 5) 上記ネットワーク接続装置は、更に処理振分部と複数のサービス処理部を備え、

上記処理振分部は、上記パケットに対するサービスの内容に基づいて、上記複数のサービス処理部のうち少なくとも 1 つに上記パケットを振り分け、

上記パケットを振り分けられたサービス処理部は、上記パケットに対するサービス処理を実行する、

ことを特徴とする付記 1 に記載のパケット中継処理装置。

(付記 6) 上記パケット中継処理装置は、更にサーバを備え、

上記サーバは、外部サービス処理部を備え、

上記処理振分部は、与えられた条件によって、上記パケットを上記サーバに転送し、

上記外部サービス処理部は、受信したパケットに対するサービスを実行する、ことを特徴とする付記 5 のパケット中継処理装置。

(付記 7) 上記パケット中継処理装置は、サーバを更に備え、

上記サーバは、パケット詳細解析部を備え、

上記ネットワーク接続装置は、更に処理振分部とサービス処理部を備え、

上記処理振分部が、与えられた条件によって上記パケットを上記パケット詳細

解析部に転送し、

上記パケット詳細解析部は、上記パケットを解析することにより上記パケットに対するサービス内容を決定し、決定した上記サービス内容を上記ネットワーク接続装置に設定し、

上記設定後、上記ネットワーク接続装置は、上記決定されたサービス内容に基づいて上記パケットを処理する、

ことを特徴とする付記 1 に記載のパケット中継処理装置。

(付記 8) 上記サービス処理部として、上記パケットのヘッダを書き換える機能を持つことを特徴とする付記 5 に記載のパケット中継処理装置。

(付記 9) 上記サービス処理部として、パケットを廃棄する機能を持つことを特徴とする付記 5 に記載のパケット中継処理装置。

(付記 10) 上記サービス処理部は、上記サーバの負荷分散のために、負荷の振分先を決定する機能を持つことを特徴とする付記 5 に記載のパケット中継処理装置。

(付記 11) 上記ネットワーク接続装置は、上記セッションに関するセッション情報を格納するセッションテーブルと、上記パケットに対するサービスを実行するための規則を記述するポリシーを格納するポリシーテーブルを備え、

上記セッション管理部は、上記パケットを受信した場合、上記パケットに含まれる情報を検索キーとして用いてセッションテーブルを検索し、

上記検索の結果、該当するセッション情報が上記セッションテーブルに登録されていない場合には、上記セッション管理部は、さらに上記パケットに含まれる情報を検索キーに基づいて、上記ポリシーテーブルから上記ポリシーを取得し、上記取得したポリシーに基づいて、上記セッション情報を上記セッションテーブルに書き込み、

上記検索の結果、該当するセッション情報が上記セッションテーブルに登録されている場合には、上記セッション管理部は、上記セッションの状態に基づいて、上記セッションテーブルに格納されたセッション情報を管理することを特徴とする付記 5 に記載のパケット中継処理装置。

(付記 12) 上記パケット中継処理装置はサーバを備え、

上記サーバは、上記ポリシーを上記ポリシーテーブルに書き込むサービス制御部を備える、

ことを特徴とする付記 1 1 に記載のパケット中継処理装置。

(付記 1 3) 上記セッションテーブルを検索する際の上記検索キーが、IP パケットの宛先及び送信元 IP アドレス、プロトコル、宛先及び送信元ポート番号、入力インタフェースを含むことを特徴とする付記 1 1 に記載のパケット中継処理装置。

(付記 1 4) 上記セッションテーブルが、上記検索キー、上記セッションの状態、適用サービス及び上記適用サービスに固有な情報をエントリとしてを持つことを特徴とする付記 1 1 に記載のパケット中継処理装置。

(付記 1 5) 上記ポリシーテーブルが、IP パケットの宛先及び送信元 IP アドレス、プロトコル、宛先及び送信元ポート番号、適用サービスと上記適用サービスに固有な情報、優先度をエントリとして持つことを特徴とする付記 1 1 に記載のパケット中継処理装置。

(付記 1 6) 上記セッション管理部は、更に、上記セッションが終了してから所定時間経過した後に、上記終了したセッションに関するセッション情報を上記セッションテーブルから削除することを特徴とする付記 1 に記載のパケット中継処理装置。

(付記 1 7) 上記ネットワーク接続装置は、更に、パケットに関する統計情報を取得するためのカウンタを備えることを特徴とする付記 1 に記載のパケット中継処理装置。

(付記 1 8) 複数のポリシーは複数のグループに分けられ、

上記ネットワーク接続装置は、更に、上記グループ毎に各ポリシーが有効であるか否かを設定することを特徴とする付記 1 1 に記載のパケット中継処理装置。

(付記 1 9) 上記ネットワーク接続装置は、更に、上記パケットのログを採取するために、上記パケットの少なくとも一部を上記サーバに転送することを特徴とする付記 1 2 に記載のパケット中継処理装置。

(付記 2 0) 上記パケットの一部は、上記パケットのヘッダであることを特徴とする付記 1 8 に記載のパケット中継処理装置。

(付記 2 1) 上記セッション情報は、上記サーバに上記パケットを転送するべきか否かを示すサーバ転送指示情報を含み、上記処理振分部は、上記サーバ転送指示情報に基づいて、上記パケットを上記サーバへの転送を行うか否かを決定する事を特徴とする付記 1 2 に記載のパケット中継処理装置。

(付記 2 2) 上記パケット詳細解析部は、更に、上記サーバに転送された上記パケットが HTTP プロトコルの GET パケットである場合、上記パケットに含まれる URL (Uniform Resource Locator) に基づいて、上記パケットに対するサービスを決定する、
ことを特徴とする付記 7 に記載のパケット中継処理装置。

(付記 2 3) 上記パケット詳細解析部は、更に、上記サーバに転送された上記パケットが FTP プロトコルの PORT 命令、或いは PASV 命令の ACK である場合、上記セッションのデータコネクションの IP アドレスとポート番号に基づいて、上記パケットに対するサービスを決定する、
ことを特徴とする付記 7 に記載のパケット中継処理装置。

(付記 2 4) 上記パケット詳細解析部は、上記サーバの負荷を分散させる処理を行う場合、上記負荷の振分先となる振分先サーバが決定されるまで、上記振分先サーバに代わって応答することを特徴とする付記 7 に記載のパケット中継処理装置。

(付記 2 5) 上記パケット詳細解析部は、上記パケットを解析することにより、上記セッションテーブルに、上記パケットに対するサービスの種類、変換用 IP アドレス及びポート番号、シーケンス番号及び ACK 番号差分を書き込む、
ことを特徴とする付記 2 1 に記載のパケット中継処理装置。

(付記 2 6) パケット中継処理装置におけるネットワーク接続装置であって、
上記ネットワーク接続装置がセッションを管理するセッション管理部と、
上記セッション管理部によるセッション管理に基づいてパケットを中継するパケット処理部を備えている
ことを特徴とするネットワーク接続装置。

(付記 2 7) 上記ネットワーク接続装置は、与えられた条件に応じて上記セッションに関するセッション情報を上記パケット中継処理装置に備えられたサーバ

に転送するサーバ転送部を備え、

上記サーバは転送された上記セッション情報により上記セッションの管理を行う

ことを特徴とする付記 2 6 のネットワーク接続装置。

(付記 2 8) 上記ネットワーク接続装置は処理振分部と複数のサービス処理部を更に備え、

上記処理振分部は、上記パケットに対するサービスの内容に基づいて、上記複数のサービス処理部のうち少なくとも 1 つに上記パケットを振り分け、

上記パケットを振り分けられたサービス処理部は、上記パケットに対するサービス処理を実行する、

ことを特徴とする付記 2 6 のネットワーク接続装置。

(付記 2 9) 上記処理振分部は、与えられた条件によって、上記パケットを上記パケット中継処理装置に備えられたサーバに転送し、上記サーバに上記パケットに対するサービス処理を実行させる

ことを特徴とする付記 2 6 のネットワーク接続装置。

(付記 3 0) 上記ネットワーク接続装置が処理振分部とサービス処理部を更に備え、

上記処理振分部は、与えられた条件によって上記パケットをパケット中継処理装置に備えられたサーバに、上記パケットに対するサービスを決定するために転送し、

上記サービス処理部は、上記サーバによるサービスの決定以後、上記サーバで決定したサービス内容に基づいて上記セッションのパケットを処理する

ことを特徴とする付記 2 6 のネットワーク接続装置。

(付記 3 1) パケットを中継する制御を、ネットワーク接続装置に備えられたコンピュータに実行させるプログラムであって、

セッションを管理し、

上記セッション管理に基づいて上記パケットを中継する

ことを含む処理を上記コンピュータに実行させることを特徴とするプログラム

(付記 3 2) 与えられた条件に応じて上記セッションに関するセッション情報を上記ネットワーク接続装置に接続されたサーバに、上記サーバに上記セッションの管理を行わせるために転送する、

ことを更に含む処理を上記コンピュータに実行させることを特徴とする付記 3 1 に記載のプログラム。

(付記 3 3) 上記パケットに対するサービスの内容に基づいて、上記サービスに対応する処理を行う装置又はプログラムセグメントに、上記パケットを振り分ける、

ことを更に含む処理を上記コンピュータに実行させることを特徴とする付記 3 1 に記載のプログラム。

(付記 3 4) 与えられた条件に応じて上記パケットを上記ネットワーク接続装置に接続されたサーバに、上記サーバに上記パケットに対するサービスを実行させるために転送する、

ことを更に含む処理を上記コンピュータに実行させることを特徴とする付記 3 3 に記載のプログラム。

(付記 3 5) 与えられた条件に応じて、上記ネットワーク接続装置に接続されたサーバへ、上記パケットに対するサービスを決定するために上記パケットを転送し、

上記サーバによる上記パケットに対するサービスの決定以後、上記決定されたサービス内容に基づきパケットを処理する

ことを含む処理を上記コンピュータに実行させること特徴とする付記 3 1 に記載のプログラム。

(付記 3 6) パケットを中継する機能を有するネットワーク接続装置に接続されたサーバに実行させるプログラムであって、

上記ネットワーク接続装置が上記パケットを処理するために、上記パケットに対するサービスを実行するための規則を記述するポリシーを上記ネットワーク接続装置に設定する、

ことを含む処理を上記サーバに実行させることを特徴とするプログラム。

(付記 3 7) 上記ネットワーク接続装置から転送された上記パケットを受信し

、受信した上記パケットに対するサービスを実行する、
ことを含む処理を上記サーバに実行させることを特徴とする付記 3 6 に記載のプログラム。

(付記 3 8) パケットを中継する機能を有するネットワーク接続装置に接続されたサーバに実行させるプログラムであって、

上記ネットワーク接続装置から転送された上記パケットを受信し、

上記パケットを解析することにより、上記パケットに対するサービスの内容を決定し、

上記決定されたサービス内容に基づいて上記ネットワーク接続装置に上記パケットを処理させるために、該決定されたサービスの内容を上記ネットワーク接続装置に設定する、

ことを含む処理を上記サーバに実行させることを特徴とするプログラム。

(付記 3 9) パケットを中継する制御を、ネットワーク接続装置に備えられたコンピュータに実行させるプログラムを記録した記録媒体であって、

セッションを管理し、

上記セッション管理に基づいて上記パケットを中継する

ことを含む処理を上記コンピュータに実行させるプログラムを記録した記録媒体。

(付記 4 0) 与えられた条件に応じて上記セッションに関するセッション情報を上記ネットワーク接続装置に接続されたサーバに、上記サーバに上記セッションの管理を行わせるために転送する、

ことを更に含む処理を上記コンピュータに実行させるプログラムを記録した付記 3 9 に記載の記録媒体。

(付記 4 1) 上記パケットに対するサービスの内容に基づいて、上記サービスに対応する処理を行う装置又はプログラムセグメントに、上記パケットを振り分ける、

ことを更に含む処理を上記コンピュータに実行させるプログラムを記録した付記 3 9 に記載の記録媒体。

(付記 4 2) 与えられた条件に応じて上記パケットを上記ネットワーク接続

装置に接続されたサーバに、上記サーバに上記パケットに対するサービスを実行させるために転送する、

ことを更に含む処理を上記コンピュータに実行させるプログラムを記録した付記 3 9 に記載の記録媒体。

(付記 4 3) 与えられた条件に応じて、上記ネットワーク接続装置に接続されたサーバへ、上記パケットに対するサービスを決定するために上記パケットを転送し、

上記サーバによる上記パケットに対するサービスの決定以後、上記決定されたサービス内容に基づきパケットを処理する

ことを更に含む処理を上記コンピュータに実行させるプログラムを記録した付記 3 9 に記載の記録媒体。

(付記 4 4) パケットを中継する機能を有するネットワーク接続装置に接続されたサーバに実行させるプログラムを記録した記録媒体であって、

上記ネットワーク接続装置が上記パケットを処理するために、上記パケットに対するサービスを実行するための規則を記述するポリシーを上記ネットワーク接続装置に設定する、

ことを含む処理を上記サーバに実行させるプログラムを記録した記録媒体。

(付記 4 5) 上記ネットワーク接続装置から転送された上記パケットを受信し、受信した上記パケットに対するサービスを実行する、

ことを更に含む処理を上記サーバに実行させるプログラムを記録した付記 4 4 に記載の記録媒体。

(付記 4 6) パケットを中継する機能を有するネットワーク接続装置に接続されたサーバに実行させるプログラムを記録した記録媒体であって、

上記ネットワーク接続装置から転送された上記パケットを受信し、

上記パケットを解析することにより、上記パケットに対するサービスの内容を決定し、

上記決定されたサービス内容に基づいて上記ネットワーク接続装置に上記パケットを処理させるために、該決定されたサービスの内容を上記ネットワーク接続装置に設定する、

ことを含む処理を上記サーバに実行させるプログラムを記録した記録媒体。

【 0 2 0 3 】

【発明の効果】

以上説明したように、本発明においては、以下の効果を得ることができる。

(1) 上記ネットワーク接続装置にセッション管理に基づくパケット中継処理部を設け、ネットワーク接続装置により、セッション管理に基づく中継処理を行うようにする。これにより、サーバのCPU使用率を下げるができる。また、ネットワーク接続装置上でセッション管理を行い、セッション開始時にセッションテーブルに出力先を登録することにより、セッションの途中でルーティングテーブルが変更されても、現在継続中のセッションについては、一貫性を保持できる。

(2) パケット中継処理装置のサーバに外部セッション管理機能を設け、ネットワーク接続装置からセッション情報を上記サーバに転送し、サーバによりセッション管理を行うことにより、セッション数がネットワーク接続装置のセッションテーブル登録数を上回った場合でも、ネットワーク接続装置で溢れた分をサーバで管理することができる。

〈3〉 処理振分部と複数のサービス処理部をサーバに比べ高速に処理できるネットワーク接続装置に配置することにより、サーバのCPUの使用率を小さくすることができるとともに、サービス処理を高速化することができる。

(4) サーバに外部サービス処理部を設け、サービス処理を、ネットワーク接続装置とサーバの両方で実行できるようにすることにより、ネットワーク接続装置2上で実現するのは困難なサービス処理をサーバで行うことができ、ネットワーク接続装置が上記決定されたサービス内容に基づき中継処理を行うようにすることにより、サーバで全ての処理を行う場合に比べ、サービス処理を高速に実現することが可能となる。

【図面の簡単な説明】

【図 1】

本発明の概要を説明する図である。

【図 2】

本発明の第 1 の実施例のパケット中継処理装置の構成を示す図である。

【図 3】

転送パケットのフレーム構成を示す図である。

【図 4】

パケット処理部の処理フローを示す図である。

【図 5】

セッション管理部の処理フローを示す図である。

【図 6】

セッションテーブルの構成例を示す図である。

【図 7】

T C P の状態遷移を示す図である。

【図 8】

T C P のセッション開始からセッション終了までの状態遷移を説明する図である。

【図 9】

U D P の状態遷移を示す図である。

【図 1 0】

本発明の第 2 の実施例のパケット中継処理装置の構成を示す図である。

【図 1 1】

第 2 の実施例のセッション管理部、外部セッション管理部における処理フローを示す図である。

【図 1 2】

本発明の第 3 の実施例のパケット中継処理装置の構成を示す図である。

【図 1 3】

第 3 実施例に係わるセッションテーブルの構成例を示す図である。

【図 1 4】

第 3 実施例にかかわるポリシーテーブルの構成例を示す図である。

【図 1 5】

本発明の第 3 の実施例のセッション管理部の処理フローを示す図である。

【図 1 6】

第 3 の実施例の処理振分部及びサービス処理部における処理フローを示す図である。

【図 1 7】

第 3 実施例におけるポリシー検索終了後の負荷分散サービスでのパケッフローを示す図である。

【図 1 8】

本発明の第 4 の実施例のパケット中継処理装置の構成を示す図である。

【図 1 9】

第 4 の実施例に係わる処理振分部、サービス処理部及び外部サービス処理部における処理の手順を示すフローチャートである。

【図 2 0】

本発明の第 5 の実施例のパケット中継処理装置の構成を示す図である。

【図 2 1】

第 5 実施例に係わるセッションテーブルの一例を示す図（その 1）である。

【図 2 2】

第 5 実施例に係わるセッションテーブルの一例を示す図（その 2）である。

【図 2 3】

第 5 実施例におけるパケット詳細解析終了後のセッションテーブルの一例を示す図（その 1）である。

【図 2 4】

第 5 実施例におけるパケット詳細解析終了後のセッションテーブルの一例を示す図（その 2）である。

【図 2 5】

詳細解析用セッションテーブルの構成例を示す図である。

【図 2 6】

詳細解析用ポリシーテーブルの構成例を示す図である。

【図 2 7】

第 5 実施例に係わるパケット中継処理装置の動作概念を示す図である。

【図 2 8】

第 5 の実施例に係わる処理振分部、サービス処理部及びパケット詳細解析部における処理の手順を示すフローチャートである。

【図 2 9】

パケット詳細解析部における処理の手順を示すフローチャートである。

【図 3 0】

URL フィルタリングの動作を説明する図である。

【図 3 1】

URL 負荷分散サービスの動作を説明する図である。

【図 3 2】

FTP フィルタリングの動作を説明する図である。

【図 3 3】

第 5 実施例における詳細解析前の URL 負荷分散サービスでのパケットフローを示す図である。

【図 3 4】

第 5 実施例における詳細解析後の URL 負荷分散サービスでのパケットフローを示す図である。

【図 3 5】

フラグテーブルのデータ構造の一例を示す図である。

【図 3 6】

コンピュータの構成図である。

【図 3 7】

コンピュータにプログラムやデータを供給する記録媒体や伝送信号を説明する図である。

【図 3 8】

サーバ及びネットワーク接続装置へのプログラムやデータのローディングを説明する図である。

【図 3 9】

従来のパケット中継処理装置の構成を示す図である。

【符合の説明】

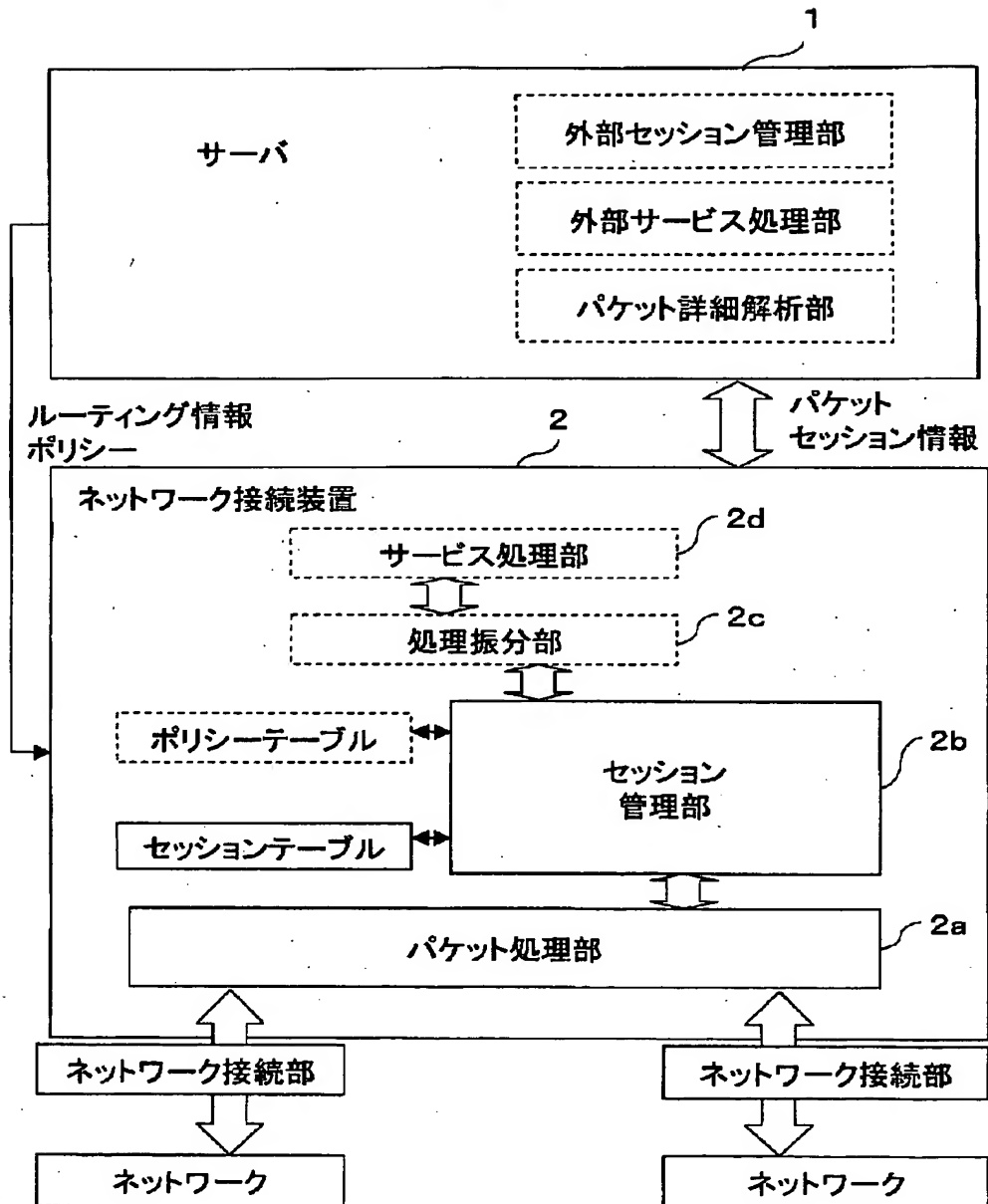
- 1 サーバ
- 2 ネットワーク接続装置
- 1 1 サーバ
- 1 2 ネットワーク制御部
- 1 3 外部セッション管理部
- 1 3 a 外部セッションテーブル
- 1 4 サービス制御部
- 1 5 外部サービス処理部
- 1 6 パケット詳細解析部
- 2 0 ネットワーク接続装置
- 2 1 パケット処理部
- 2 2 セッション管理部
- 2 2 a セッションテーブル
- 2 2 a' セッションテーブル
- 2 3 ルーティング処理部
- 2 3 a ルーティングテーブル
- 2 4 サーバ転送部
- 2 5 ポリシーテーブル
- 2 6 処理振分部
- 2 7 サービス処理部
- 3 0 ネットワーク接続部
- 3 1 制御情報通信部
- 3 2 セッション情報通信部
- 3 3 パケット通信路
- 4 0 コンピュータ
- 4 1 C P U
- 4 2 メモリ

- 4 3 入力装置
- 4 4 出力装置
- 4 5 外部記憶装置
- 4 6 媒体駆動装置
- 4 7 ネットワークインターフェース
- 4 8 バス
- 4 9 可搬記録媒体
- 5 0 データベース
- 5 1 回線
- A 矢印
- P パケット
- S ステップ

【書類名】 図面

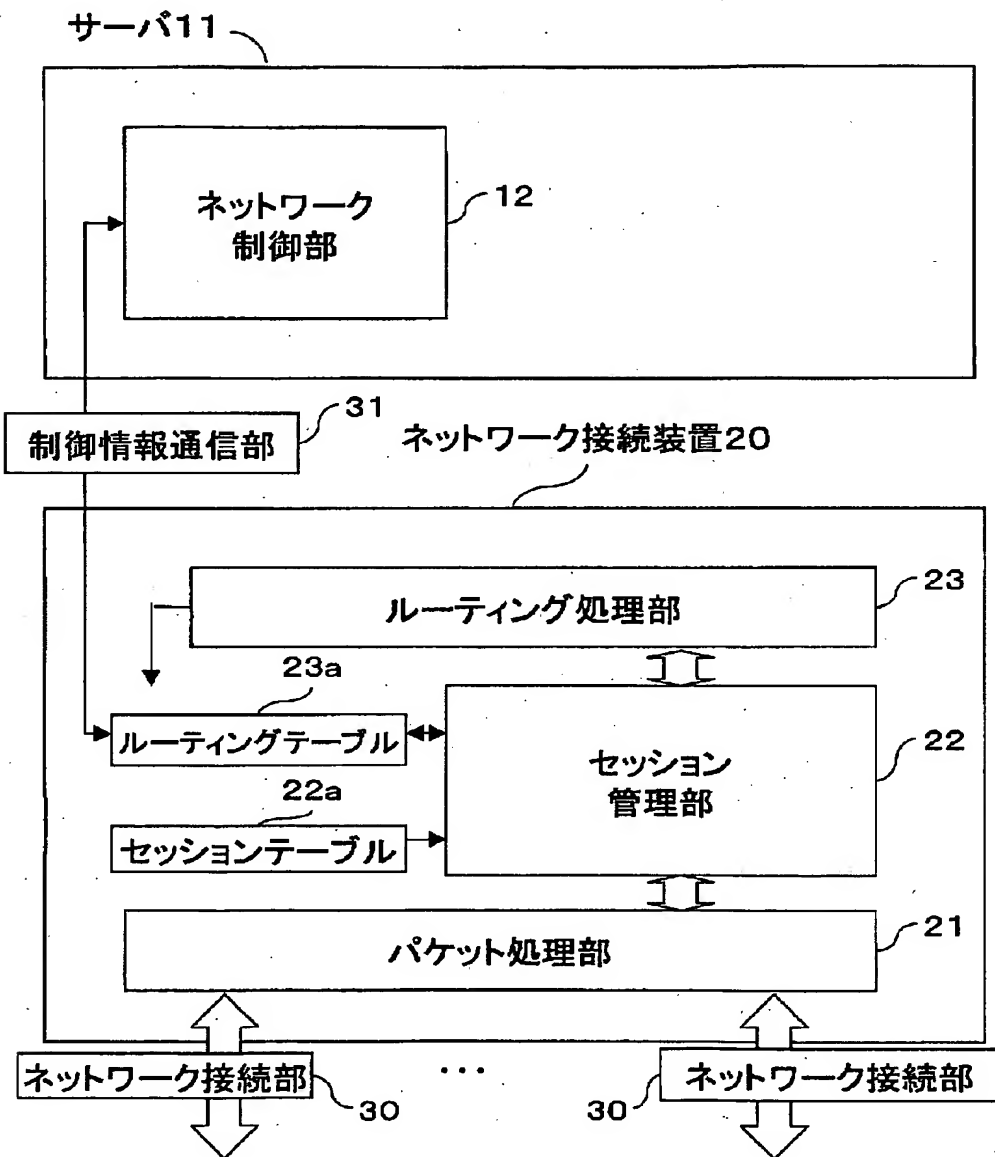
【図 1】

本発明の概要を示す図



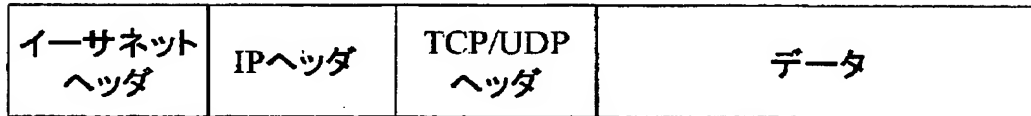
【図 2】

本発明の第1の実施例のパケット中継処理装置の構成を示す図



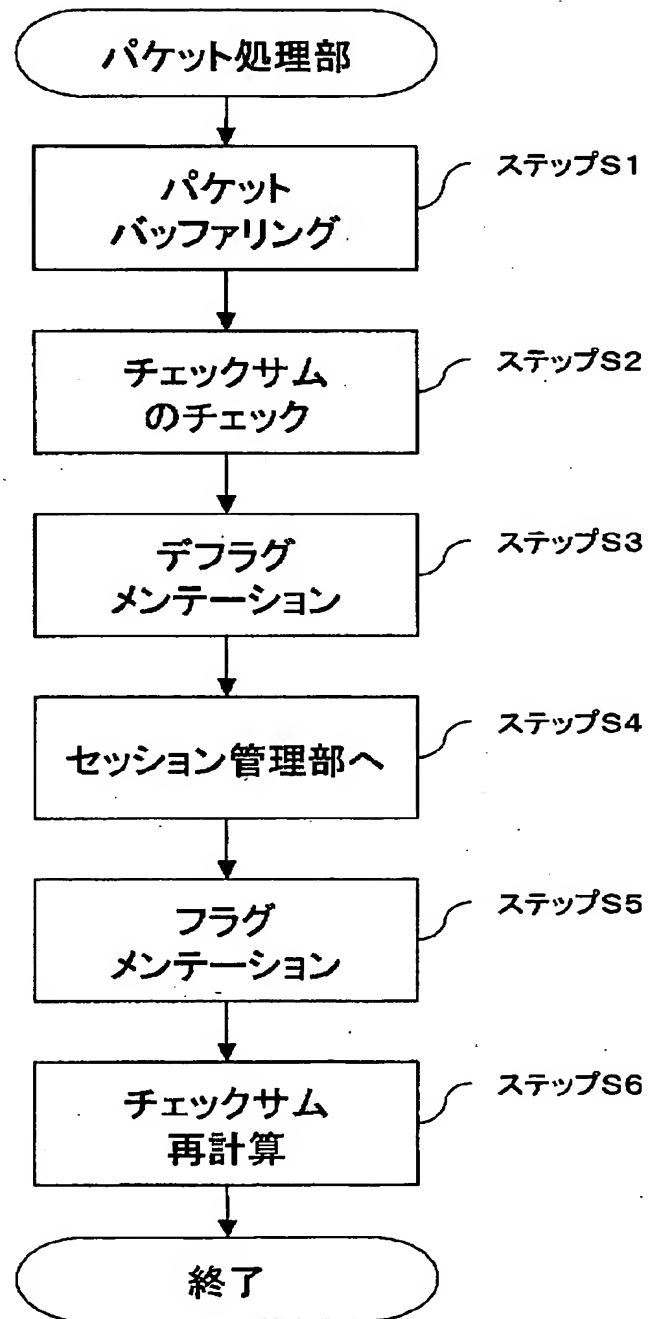
【図3】

転送パケットのフレーム構成を示す図



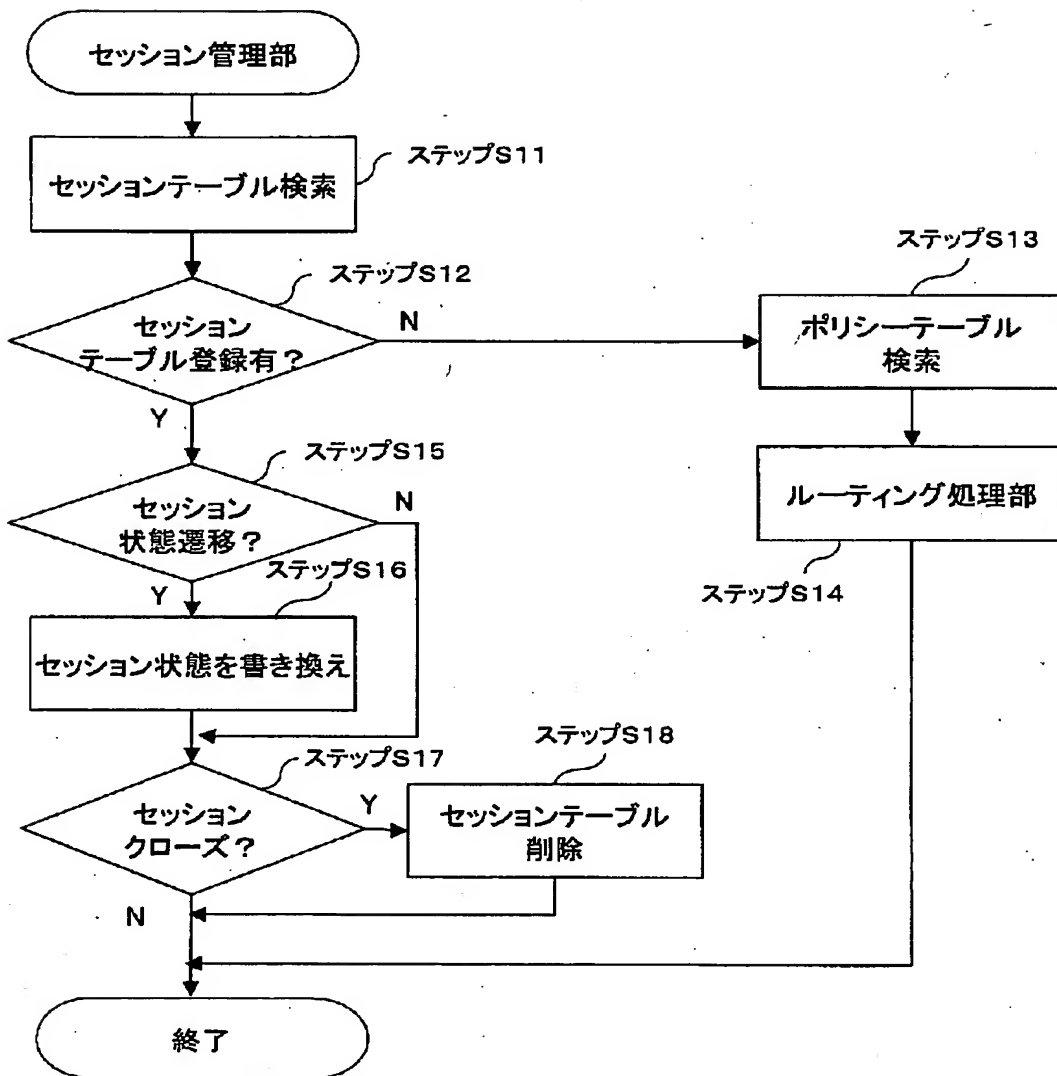
【図4】

パケット処理部の処理フローを示す図



【図5】

セッション管理部の処理フローを示す図



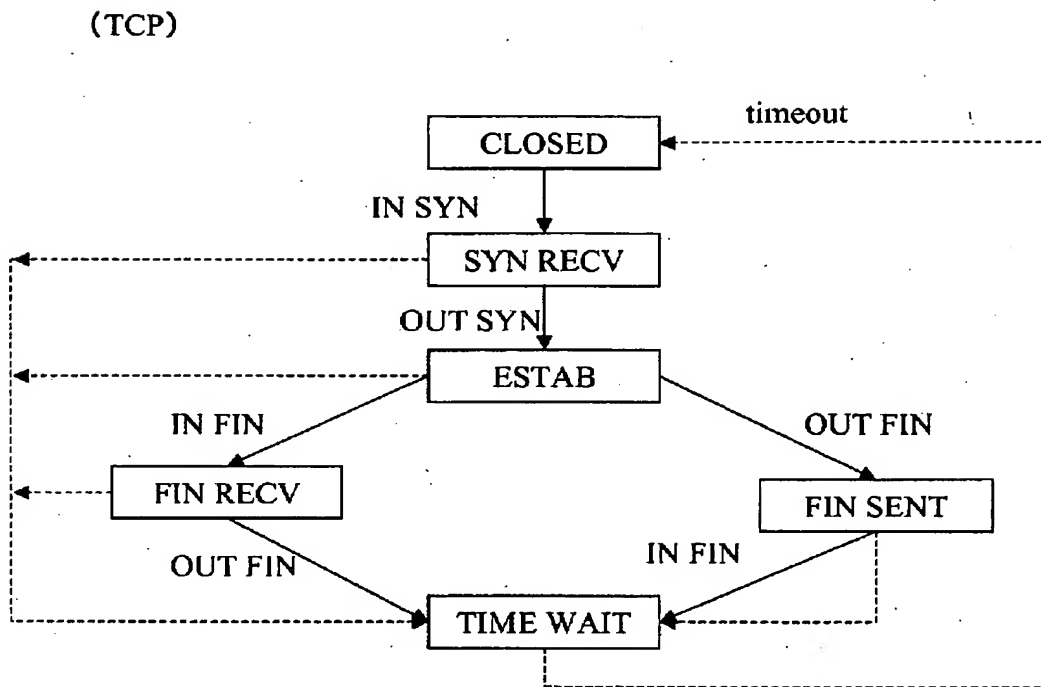
【図 6】

セッションテーブルの構成例を示す図

セッションID	セッション検索キー					セッション状態	出力先
	送信元 IP アドレス	送信元ポート番号	プロトコル	宛先 IP アドレス	宛先ポート番号		
0	192.168.100.14	13200	TCP	192.168.10.5	8080	ESTAB	
1	192.168.10.5	8080	TCP	192.168.100.14	13200	ESTAB	
2	192.168.100.100	http	TCP	10.25.1.230	9250	IN SYN	
3	10.25.1.230	9250	TCP	192.168.100.75	http	IN SYN	

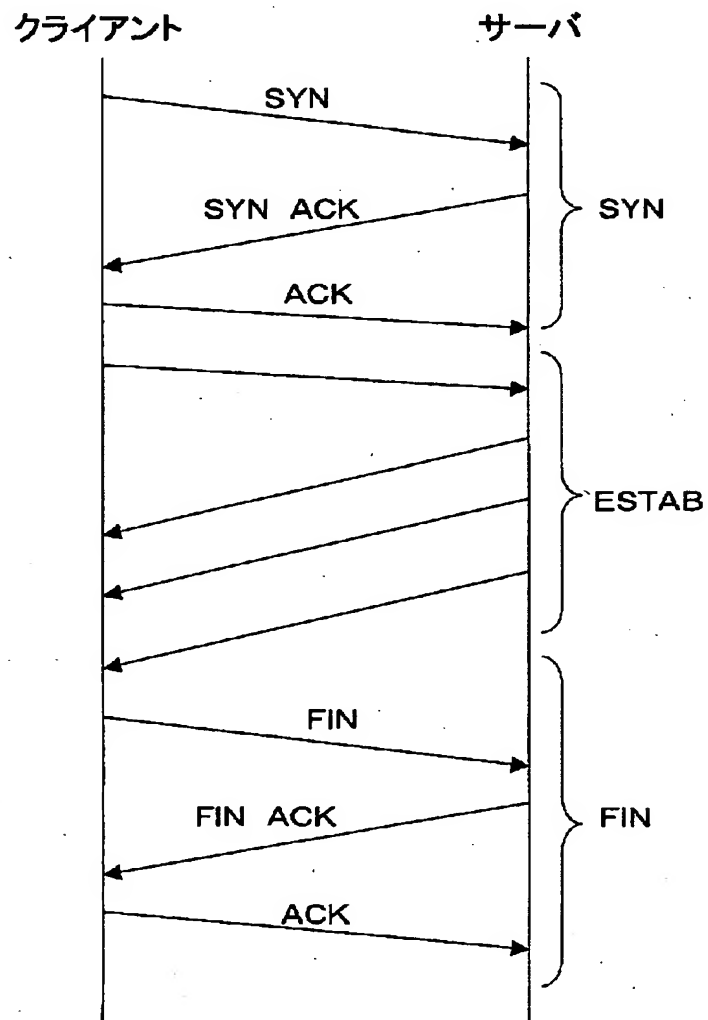
【図 7】

TCPの状態遷移を示す図



【図 8】

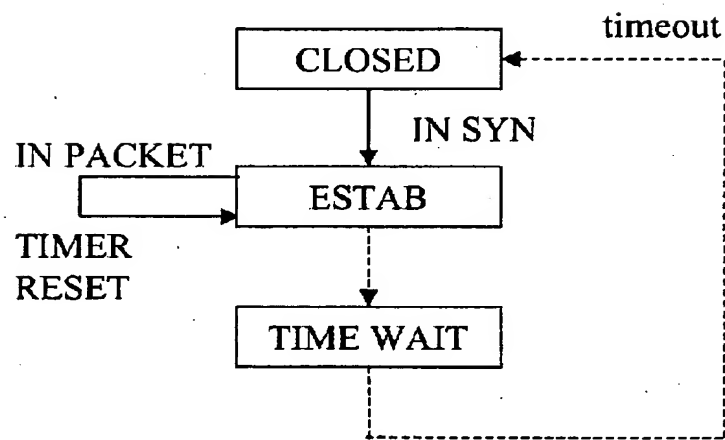
TCPのセッション開始から終了までの状態遷移を説明する図



【図9】

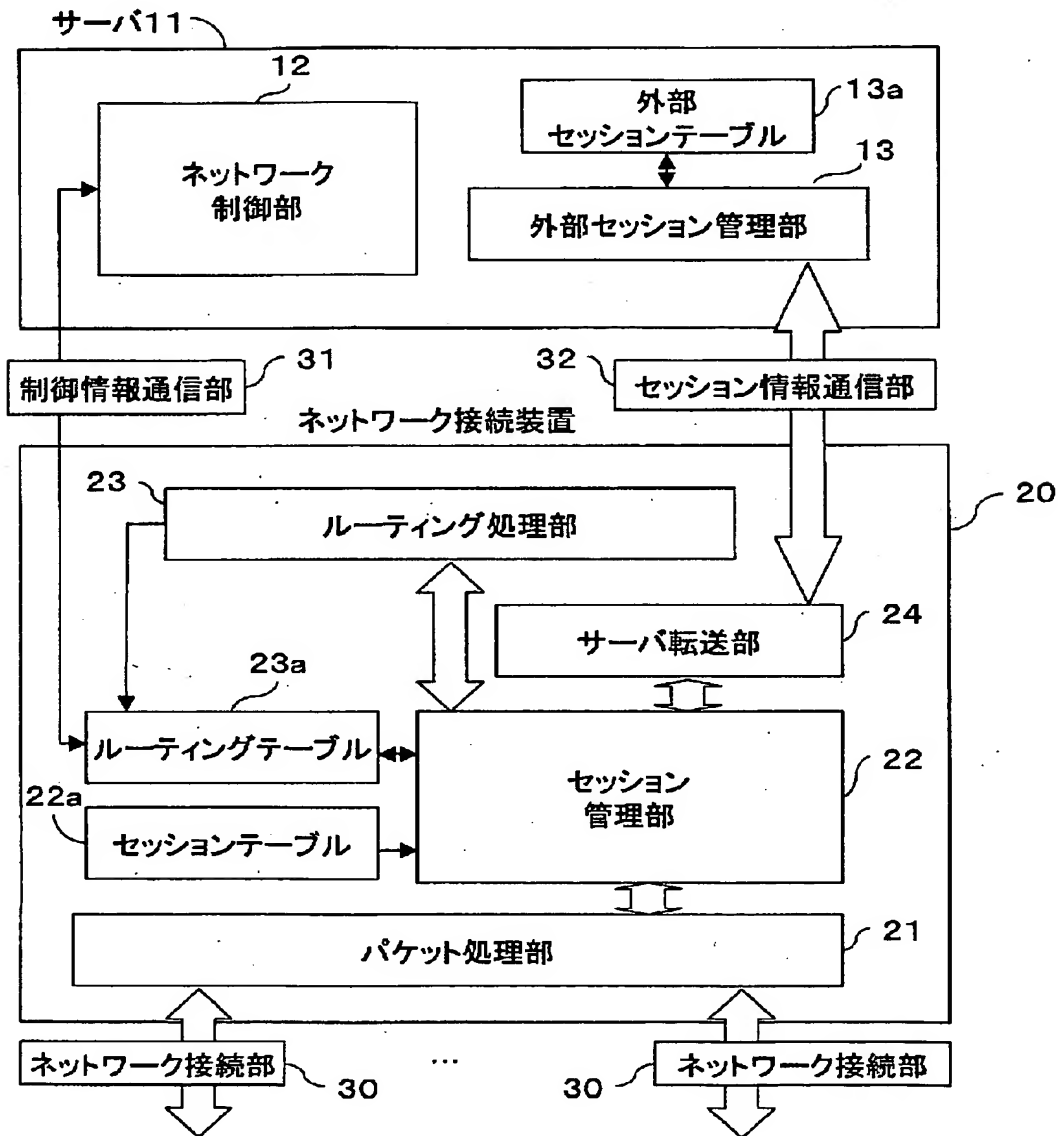
UDPの状態遷移を示す図

(UDP)



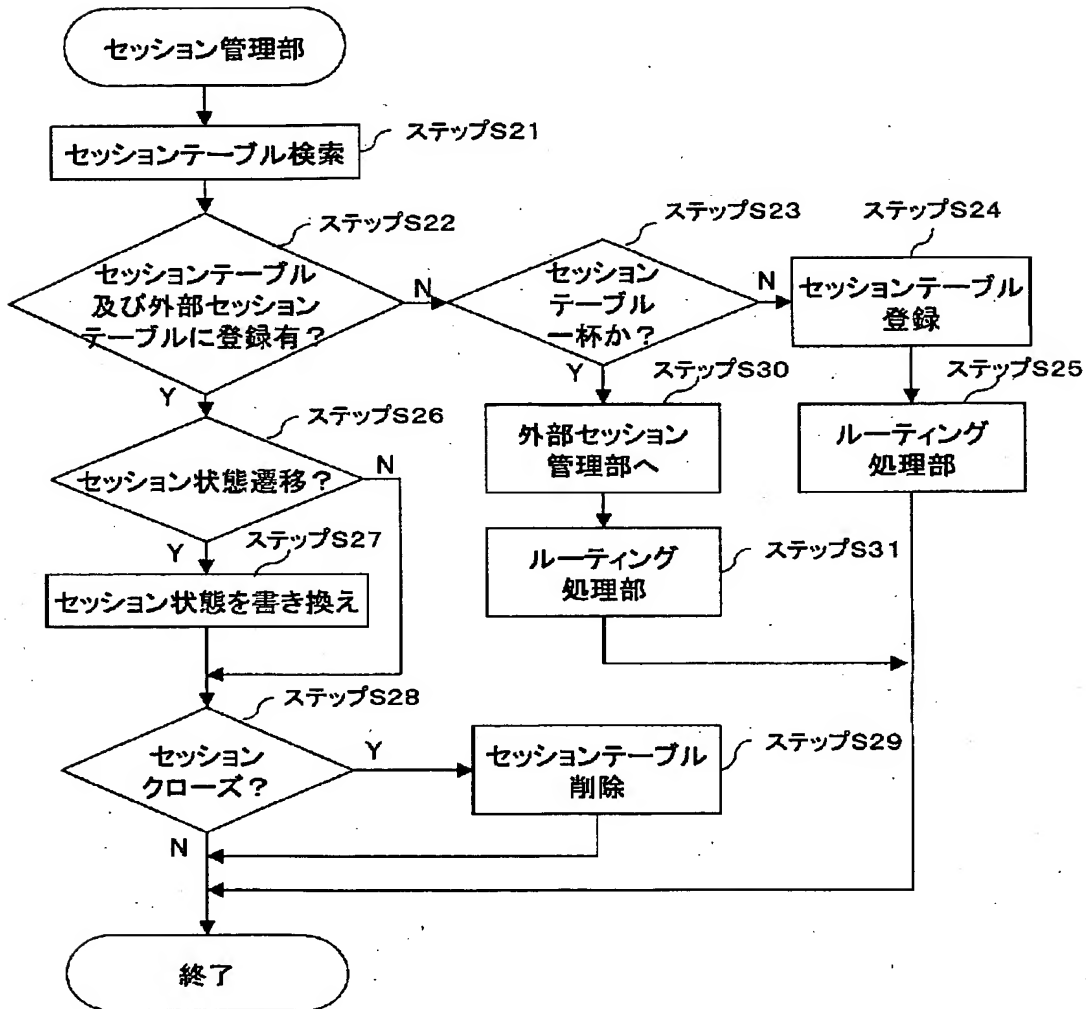
【図10】

本発明の第2の実施例のパケット中継処理装置の構成を示す図



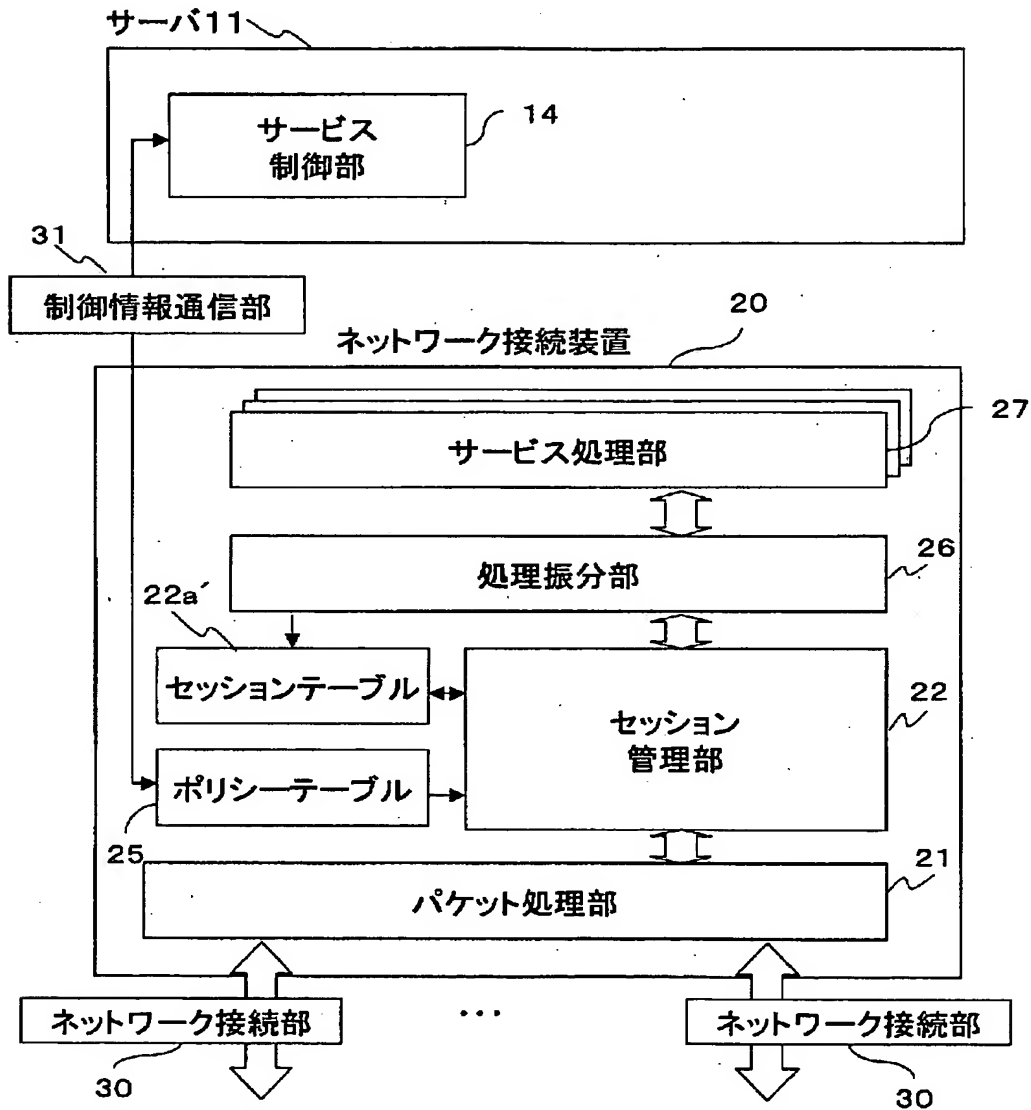
【図 11】

第2の実施例のセッション管理部、
外部セッション管理部における処理フローを示す図



【図 1 2】

本発明の第3の実施例のパケット中継処理装置の構成を示す図



【図 13】

第3実施例に係るセッションテーブルの構成例を示す図

セッションID		0	1	2	3
セッション検索キー	送信元IPアドレス	192.168.100.14	192.168.10.5	192.168.100.100	10.25.1.230
	送信元ポート番号	13200	8080	http	9250
	プロトコル	TCP	TCP	TCP	TCP
	宛先IPアドレス	192.168.10.5	192.168.100.14	10.25.1.230	192.168.100.75
	宛先ポート番号	8080	13200	9250	http
	入力インタフェース	0	1	0	1
セッション状態		ESTAB	ESTAB	IN SYN	IN SYN
出力先インタフェース		1	0	1	0
適用サービスタイプ		フィルタリング通過	フィルタリング通過	ヘッダ書換	ヘッダ書換
固有情報		-	-	Src:192.168.100.75	Dst:192.168.100.100
一貫性保持時間(ms)		1000	1000	3000	3000
イベントフラグ(パケット)		OFF	OFF	OFF	OFF
イベントフラグ(ヘッダ)		ON	ON	OFF	OFF

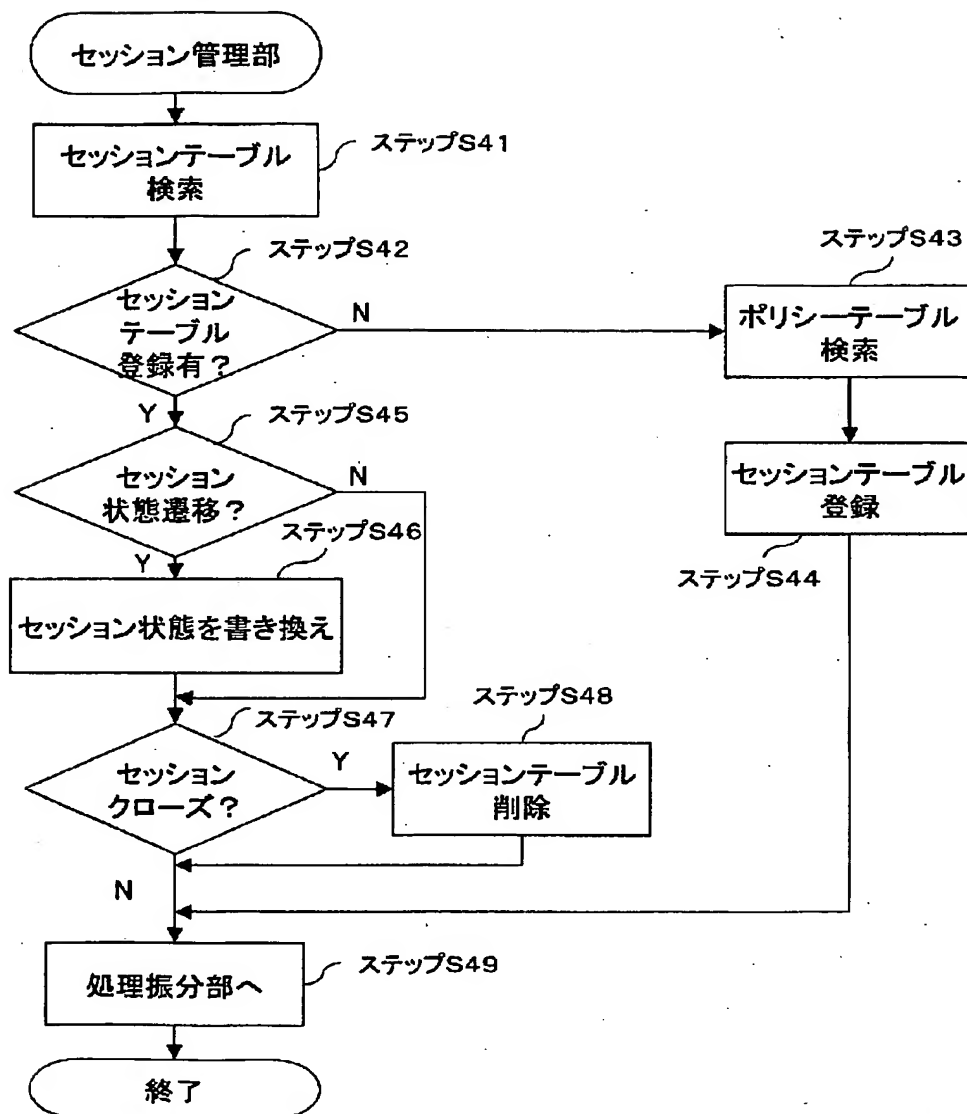
【図 1 4】

第3実施例に係るポリシーテーブルの構成例を示す図

ポリシーID		0	1
ポリシー検索キー	送信元IPアドレス	Any	Any
	送信元ポート番号	Any	Any
	プロトコル	Any	TCP
	宛先IPアドレス	GW	192.168.100.75
	宛先ポート番号	Any	http
適用サービスタイプ		フロッピング廃棄	負荷分散
サービス固有情報		-	振り分け先 1: 192.168.100.100 振り分け先 2: 192.168.100.110 振り分け先 3: 192.168.100.120 振り分け先 4: 192.168.100.130 振り分け方法: ラウンドロビン
優先度		5000	1000
グループID		6	32
イベントフラグ(パケット)		OFF	OFF
イベントフラグ(ヘッダ)		ON	OFF
一貫性保持時間 (ms)		1000	3000
ポリシーヒット数		2	2

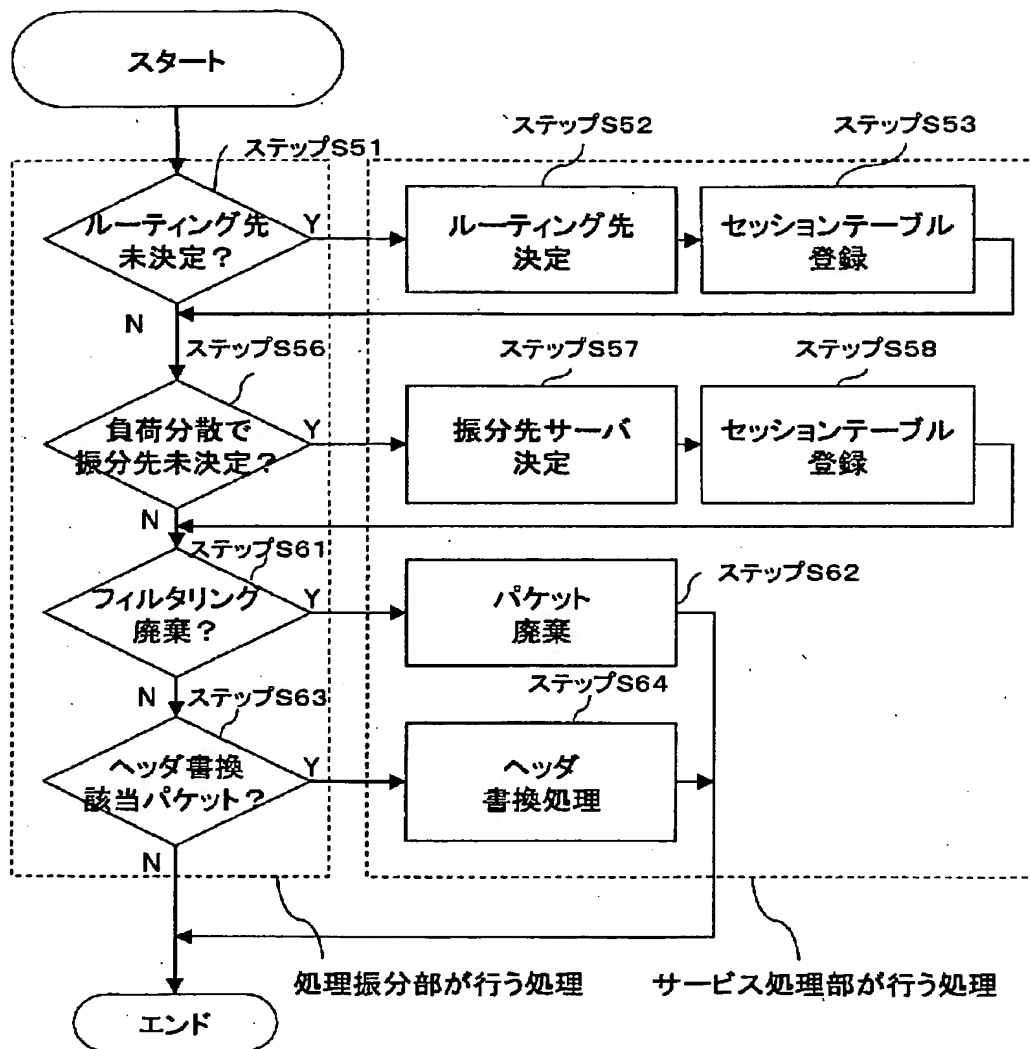
【図15】

本発明の第3の実施例のセッション管理部の処理フローを示す図



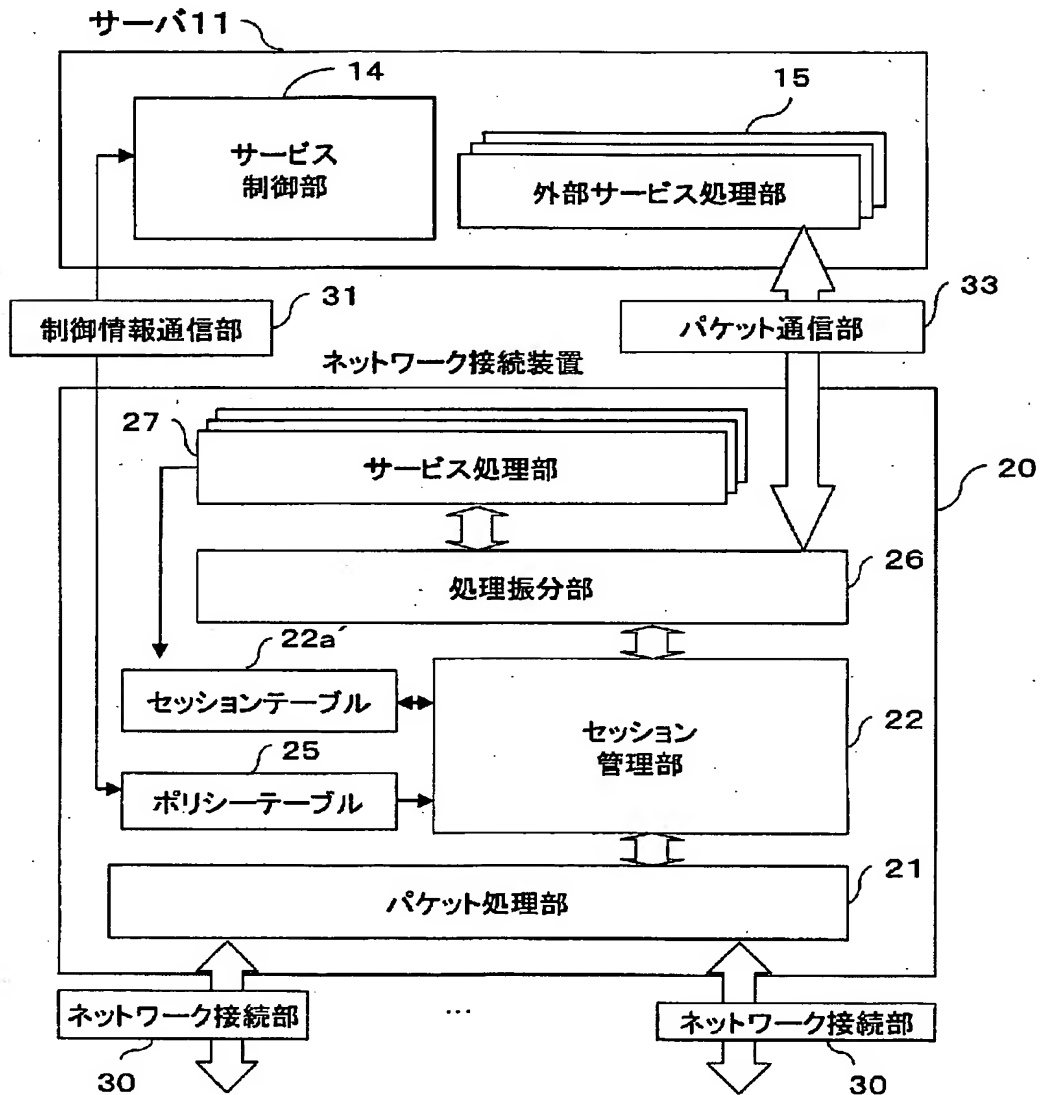
【図16】

第3実施例に係る処理振分部及び
サービス処理部の処理フローを示す図



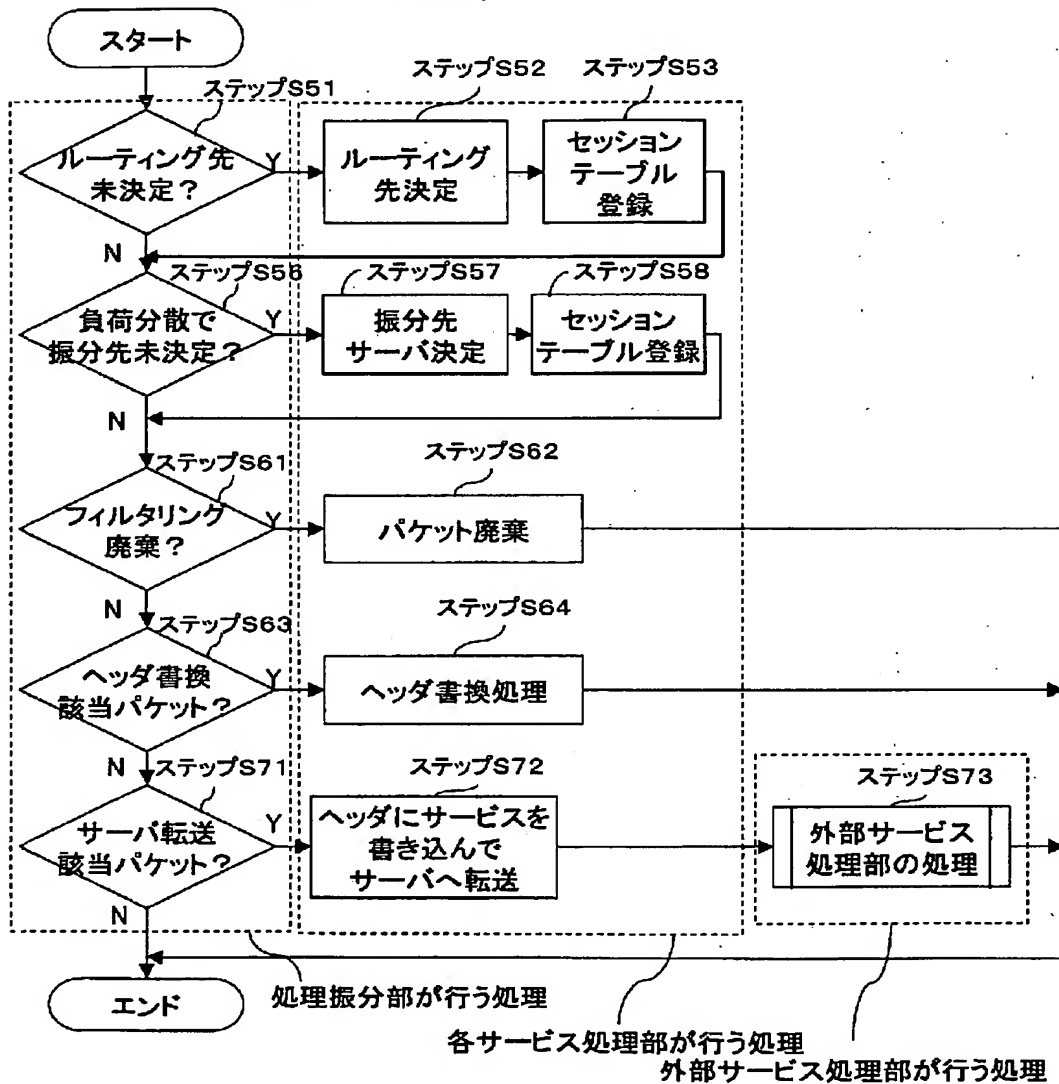
【図18】

本発明の第4の実施例のパケット中継処理装置の構成を示す図



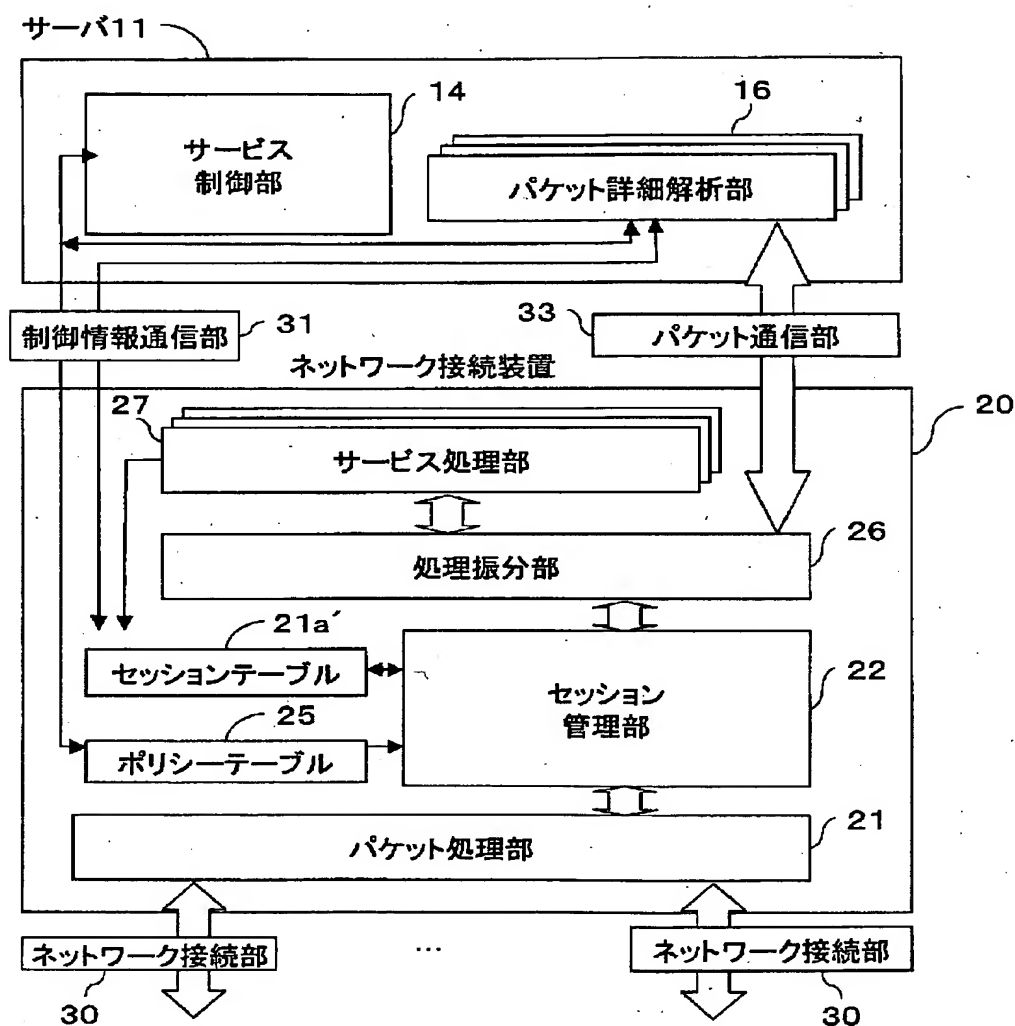
【図19】

第4実施例に係る処理振分部、
サービス処理部及び外部サービス処理部における
処理の手順を示すフローチャート



【図 20】

本発明の第5の実施例のパケット中継処理装置の構成を示す図



【図 2 1】

第5実施例におけるセッションテーブルの一例を示す図(その1)

(URL 負荷分散、および URL フィルタリング)

セッションID		0	1	2	3	4	5
セッション検索キー	送信元IPアドレス	192.168.50.5	192.168.1.5	192.168.30.30	192.168.200.1	192.168.200.1	192.168.200.10
	送信元ポート番号	16321	8080	11950	http	3333	8080
セッション検索キー	プロトコル	TCP	TCP	TCP	TCP	TCP	TCP
	宛先IPアドレス	192.168.1.5	192.168.50.5	192.168.200.1	192.168.30.30	192.168.200.10	192.168.200.1
セッション検索キー	宛先ポート番号	8080	16321	http	11950	8080	3333
	入力インタフェース	0	1	0	Server	Server	1
セッション検索キー	セッション状態	IN SYN	IN SYN	ESTAB	ESTAB	IN SYN	IN SYN
	出力先インタフェース	1	0	-	0	1	-
適用サービスタイプ	サーバ転送:ON	サーバ転送:ON	サーバ転送:ON	サーバ転送:ON	サーバ転送:ON	サーバ転送:ON	サーバ転送:ON
	URL フィルタリング	URL フィルタリング	URL フィルタリング	URL 負荷分散	URL 負荷分散	URL 負荷分散	URL 負荷分散
固有情報	変換用送信元IPアドレス	-	-	-	-	-	-
	変換用送信元ポート番号	-	-	-	-	-	-
	変換用宛先IPアドレス	-	-	-	-	-	-
	変換用宛先ポート番号	-	-	-	-	-	-
	シーケンス番号差分	-	-	-	-	-	-
ACK番号差分		-	-	-	-	-	-
一貫性保持時間(ms)		1000	1000	3000	3000	3000	3000
イベントフラグ(パケット)		OFF	OFF	OFF	OFF	OFF	OFF
イベントフラグ(ヘッダ)		OFF	OFF	OFF	OFF	OFF	OFF

URL 負荷分散

【図 2 2】

第5実施例におけるセッションテーブルの一例を示す図(その2)

(FTP フィルタリング)

セッションID		6	7
セッション検索キー	送信元IPアドレス	192.168.2.100	192.168.25.250
	送信元ポート番号	3001	21
	プロトコル	TCP	TCP
	宛先IPアドレス	192.168.25.250	192.168.2.100
	宛先ポート番号	21	3001
	入力インタフェース	0	1
セッション状態		IN SYN	IN SYN
出力先インタフェース		1	0
適用サービスタイプ		サーバ転送:ON FTP フィルタリング	サーバ転送:ON FTP フィルタリング
固有情報	変換用送信元IPアドレス	-	-
	変換用送信元ポート番号	-	-
	変換用宛先IPアドレス	-	-
	変換用宛先ポート番号	-	-
	シーケンス番号差分	-	-
	ACK番号差分	-	-
貫性保持時間(ms)		1000	1000
イベントフラグ(パケット)		OFF	OFF
イベントフラグ(ヘッダ)		OFF	OFF

【図 23】

第5実施例におけるパケット詳細解析終了後のセッションテーブルの一例を示す図(その1)(URL負荷分散、およびURLフィルタリング)

セッションID	0	1	2	5
送信元IPアドレス	192.168.50.5	192.168.1.5	192.168.30.30	192.168.200.10
送信元ポート番号	16321	8080	11950	8080
プロトコル	TCP	TCP	TCP	TCP
宛先IPアドレス	192.168.1.5	192.168.50.5	192.168.200.1	192.168.200.1
宛先ポート番号	8080	16321	http	3333
入力インタフェース	0	1	0	1
セッション状態	ESTAB	ESTAB	ESTAB	ESTAB
出力先インタフェース	1	0	1	0
適用サービスタイプ	サーバ転送:OFF フィルタリング:通過	サーバ転送:OFF フィルタリング:通過	サーバ転送:OFF ヘッダ書換	サーバ転送:OFF ヘッダ書換
変換用送信元IPアドレス	-	-	-	192.168.200.1
変換用送信元ポート番号	-	-	-	http
変換用宛先IPアドレス	-	-	192.168.200.10	192.168.30.30
変換用宛先ポート番号	-	-	8080	11950
シーケンス番号差分	-	-	2394	14733
ACK番号差分	-	-	54654	8002
貫性保持時間(ms)	1000	1000	3000	3000
イベントフラグ(パケット)	OFF	OFF	OFF	OFF
イベントフラグ(ヘッダ)	OFF	OFF	OFF	OFF

【図 24】

第5実施例におけるパケット詳細解析終了後の
セッションテーブルの一例を示す図(その2)(FTPフィルタリング)

セッションID	6	7	8	9
送信元IPアドレス	192.168.2.100	192.168.25.250	192.168.2.100	192.168.25.250
送信元ポート番号	3001	21	3002	20
プロトコル	TCP	TCP	TCP	TCP
宛先IPアドレス	192.168.25.250	192.168.2.100	192.168.25.250	192.168.2.100
宛先ポート番号	21	3001	20	3002
入カインタフェース	0	1	0	1
セッション状態	ESTAB	ESTAB	ESTAB	ESTAB
出力先インタフェース	1	0	1	0
運用サービスタイプ	サーバ転送:ON FTPフィルタリング	サーバ転送:ON FTPフィルタリング	サーバ転送:ON FTPフィルタリング	サーバ転送:ON FTPフィルタリング
変換用送信元IPアドレス	-	-	-	-
変換用送信元ポート番号	-	-	-	-
変換用宛先IPアドレス	-	-	-	-
変換用宛先ポート番号	-	-	-	-
シーケンス番号差分	-	-	-	-
ACK番号差分	-	-	-	-
一貫性保持時間(ms)	1000	1000	3000	3000
イベントフラグ(パケット)	OFF	OFF	OFF	OFF
イベントフラグ(ヘッダ)	OFF	OFF	OFF	OFF

制御コネクション

データコネクション

【図 25】

詳細解析用セッションテーブルの構成例を示す図

セッションID	0	1	2	3	4	5	6	7
セッション検索キー	送信元 IPアドレス	192.168.50.5	192.168.1.5	192.168.30.30	192.168.200.1	192.168.200.1	192.168.200.10	192.168.25.250
	送信元 ポート番号	16321	8080	11950	http	3333	8080	3001
	プロトコル	TCP	TCP	TCP	TCP	TCP	TCP	TCP
	宛先 IPアドレス	192.168.1.5	192.168.50.5	192.168.200.1	192.168.30.30	192.168.200.10	192.168.200.1	192.168.2.100
	宛先 ポート番号	8080	16321	http	11950	8080	3333	21
セッション状態	入力 インターフェイス	0	1	0	Server	Server	1	0
	セッション状態	IN SYN	IN SYN	ESTAB	ESTAB	IN SYN	IN SYN	IN SYN
関連セッション	関連セッション	-	-	4	5	2	3	-
	適用サービスタイプ	サーバ転送:ON URLフィルタリング	サーバ転送:ON URLフィルタリング	サーバ転送:ON URL負荷分散	サーバ転送:ON URL負荷分散	サーバ転送:ON URL負荷分散	サーバ転送:ON URL負荷分散	サーバ転送:ON FTPファイルリンク

【図 2 6】

詳細解析用ポリシーテーブルの構成例を示す図

URI フィルタリング用 URL テーブル

URL	通過/廃棄
<u>www.xxx.com</u>	廃棄
www2.yyy.co.jp	廃棄
bbb.ne.jp/~abc	廃棄
aaa.bbb.or.jp	廃棄

FTP フィルタリング用テーブル

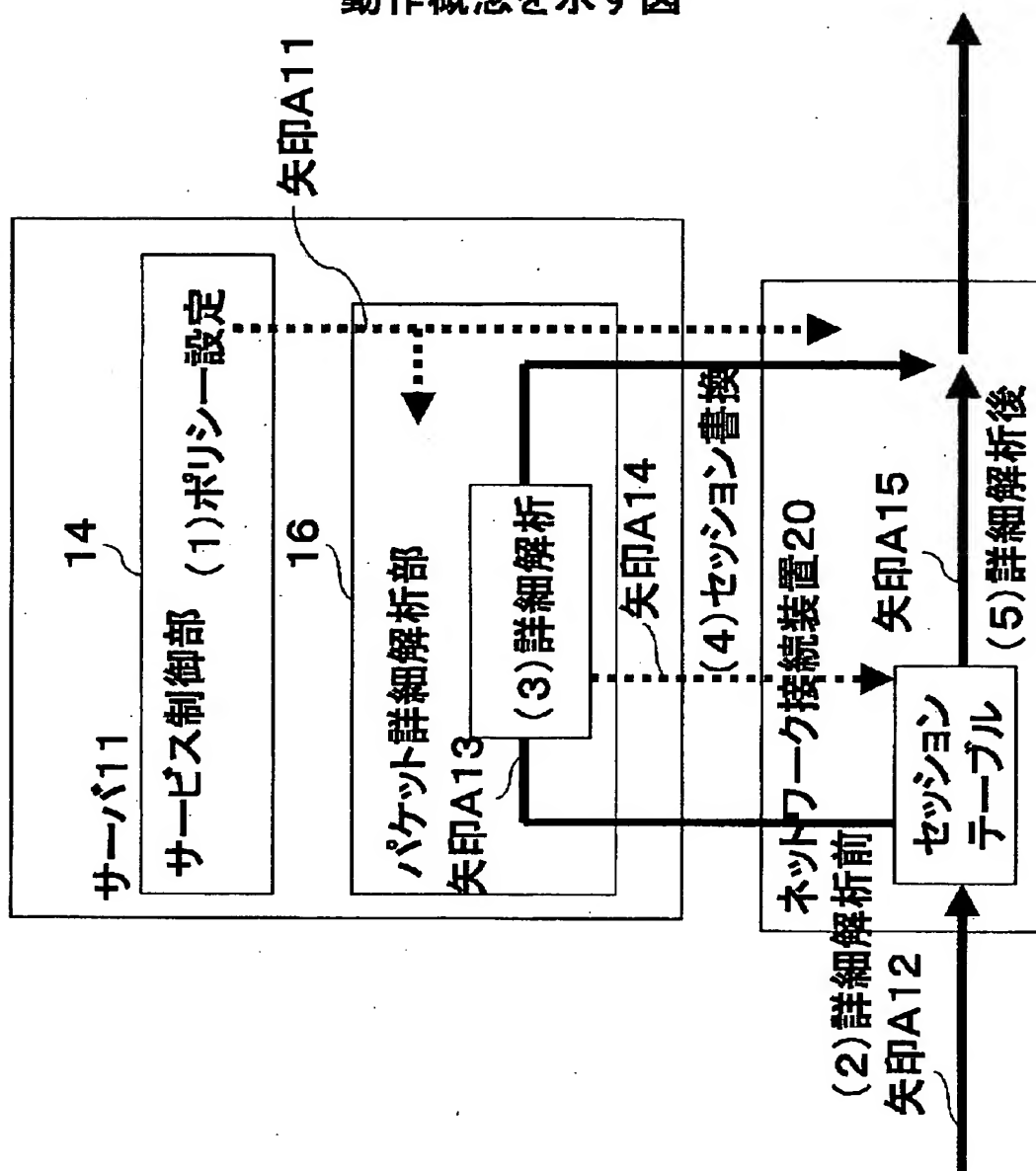
IP アドレス: ポート番号	通過/廃棄
192.168.1.5: Any	通過
192.168.2.100: Any	通過
192.168.150.*: Any	通過
192.168.250.*: Any	通過

URL 負荷分散用テーブル

URL	振分先
<u>www.aaa.com</u>	振分先 1: 192.168.200.10 振分先 2: 192.168.200.11 振分先 3: 192.168.200.12 振分先 4: 192.168.200.13 振分方法: ラウンドロビン
<u>www.bbb.co.jp</u>	振分先 1: 192.168.200.20 振分先 2: 192.168.200.21 振分先 3: 192.168.200.22 振分方法: ラウンドロビン
<u>www.ccc.ne.jp</u>	振分先 1: 192.168.200.30 振分先 2: 192.168.200.31 振分方法: ラウンドロビン
<u>www.ddd.ne.jp/~abc</u>	振分先 1: 192.168.200.40 振分先 2: 192.168.200.41 振分先 3: 192.168.200.42 振分先 4: 192.168.200.43 振分方法: ラウンドロビン

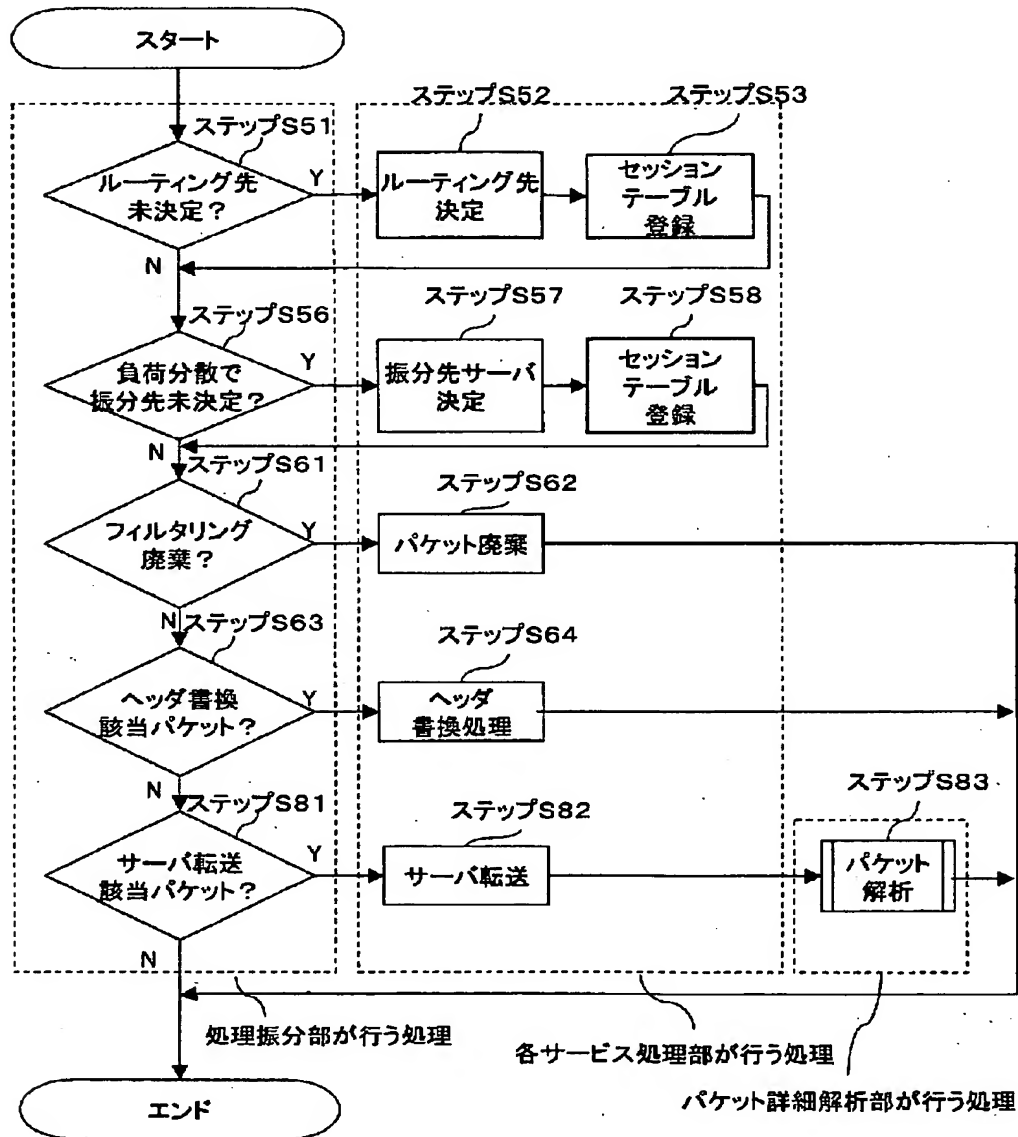
【图 2 7】

第5実施例に係るパケット中継処理装置の動作概念を示す図



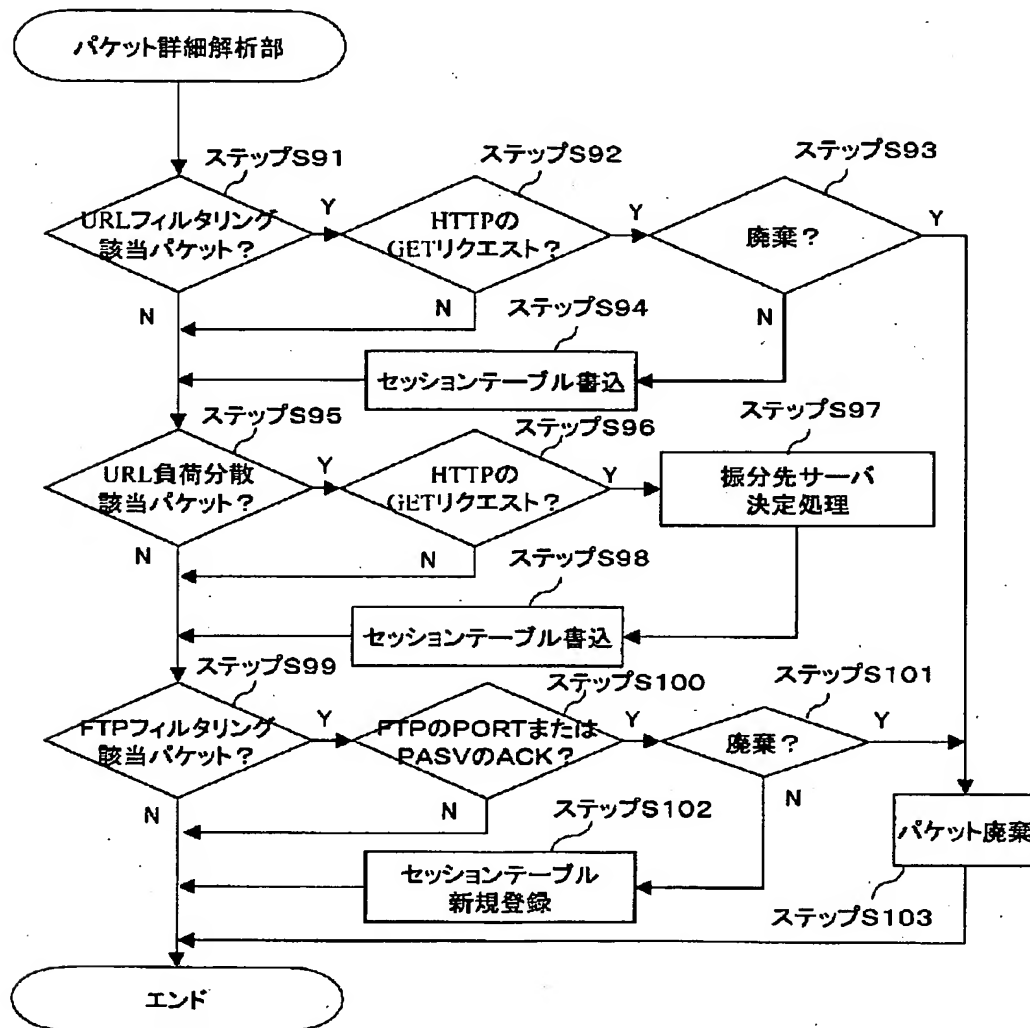
【図 28】

第5実施例に係る処理振分部、サービス処理部及び
パケット詳細解析部における処理の手順を示すフローチャート



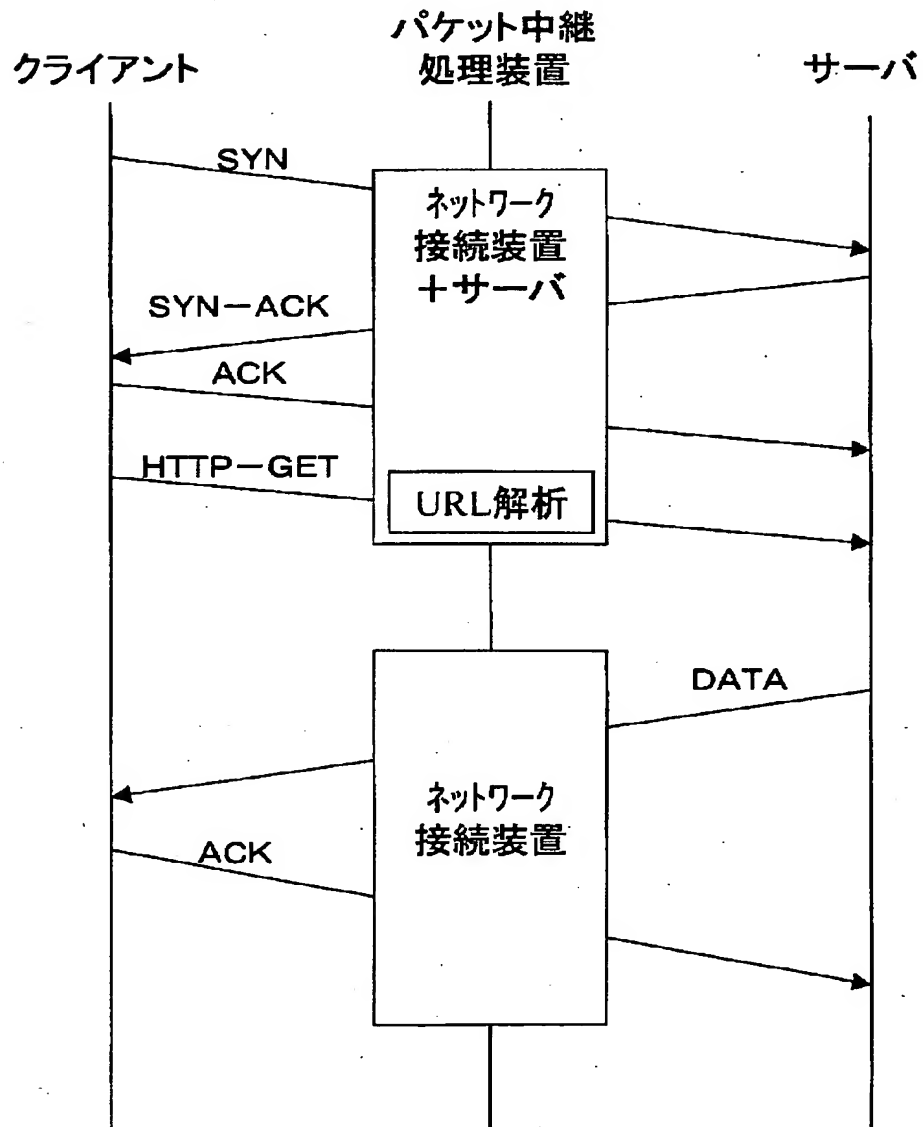
【図 29】

パケットの詳細解析における処理の手順を示すフローチャート



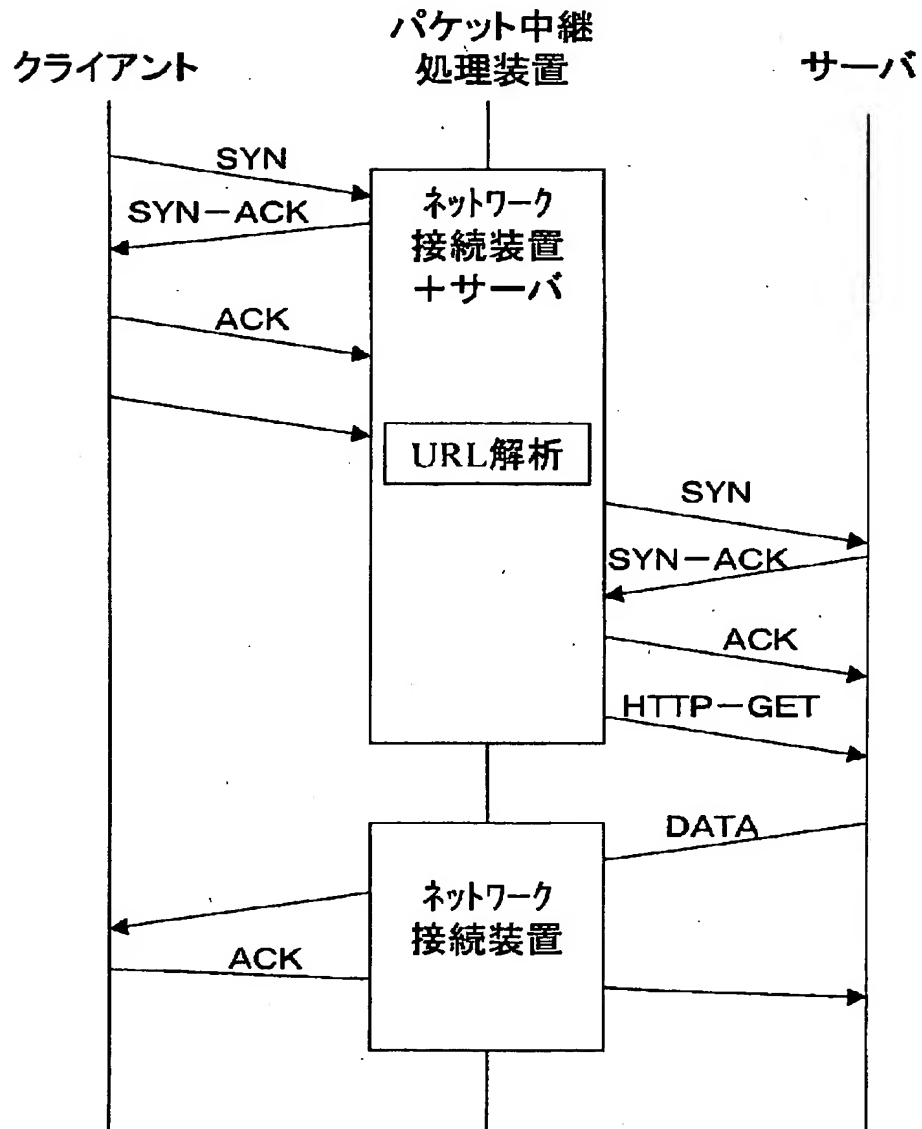
【図 30】

URLフィルタリングの動作を説明する図



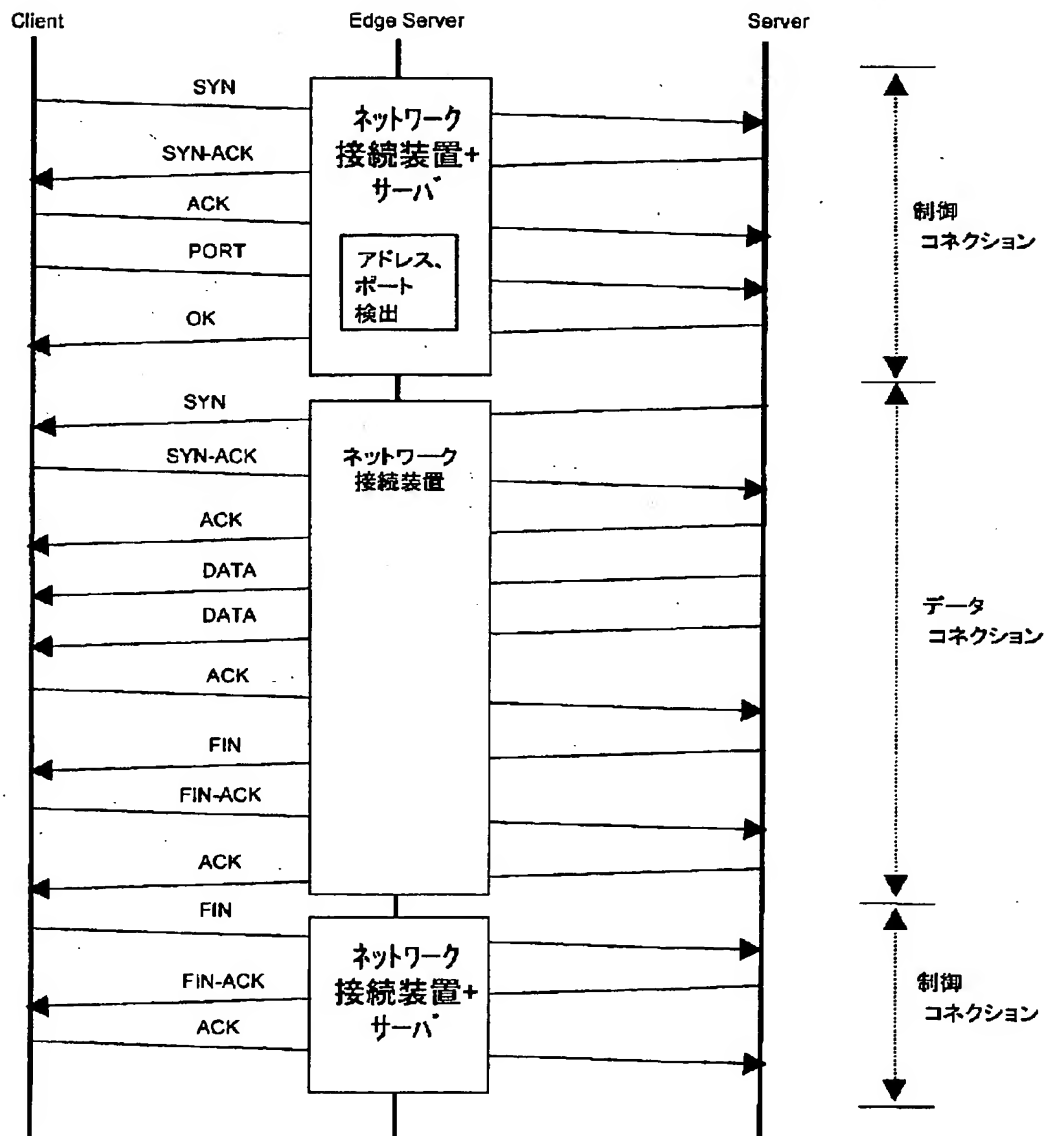
【図 3 1】

URL 負荷分散の動作を説明する図



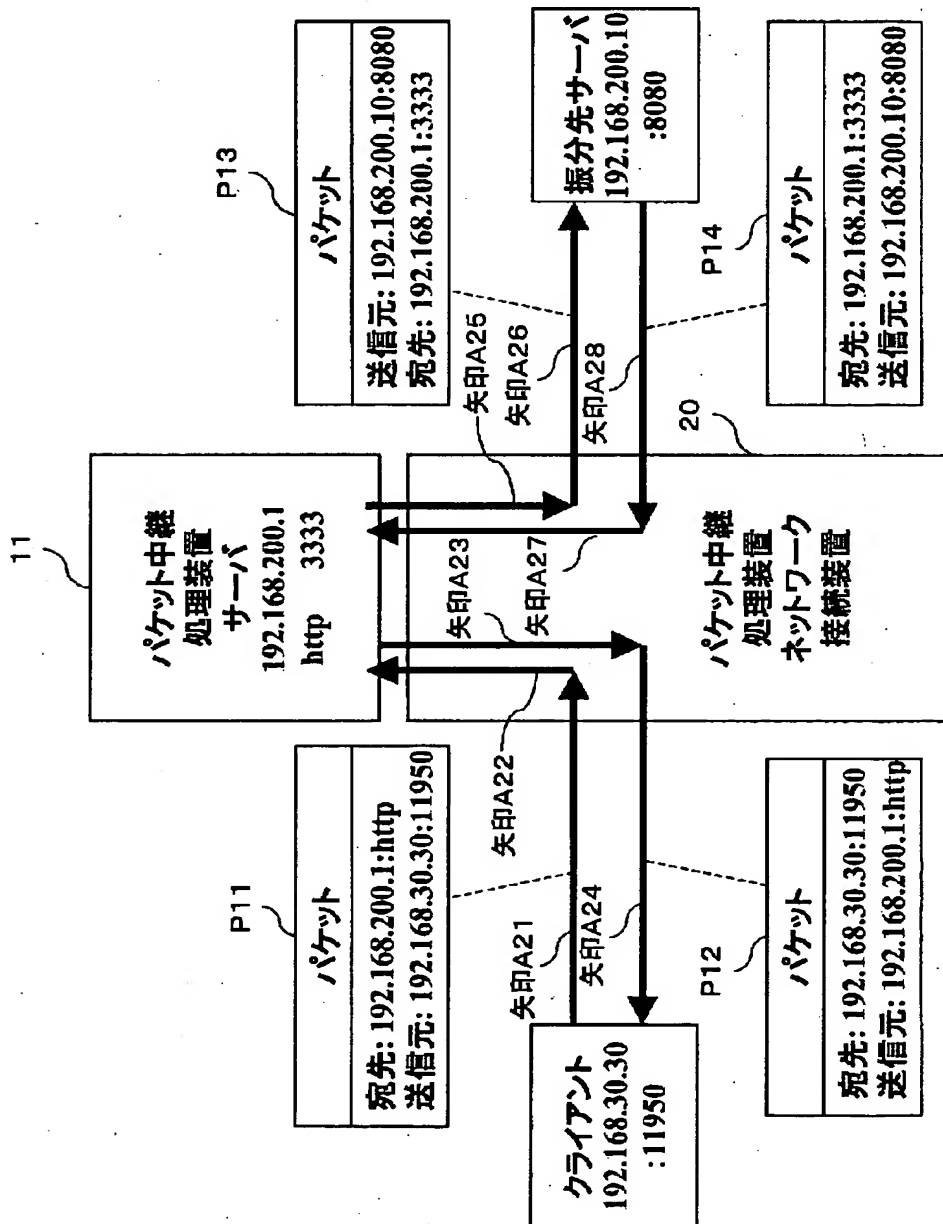
【図 3 2】

FTPフィルタリングの動作を説明する図



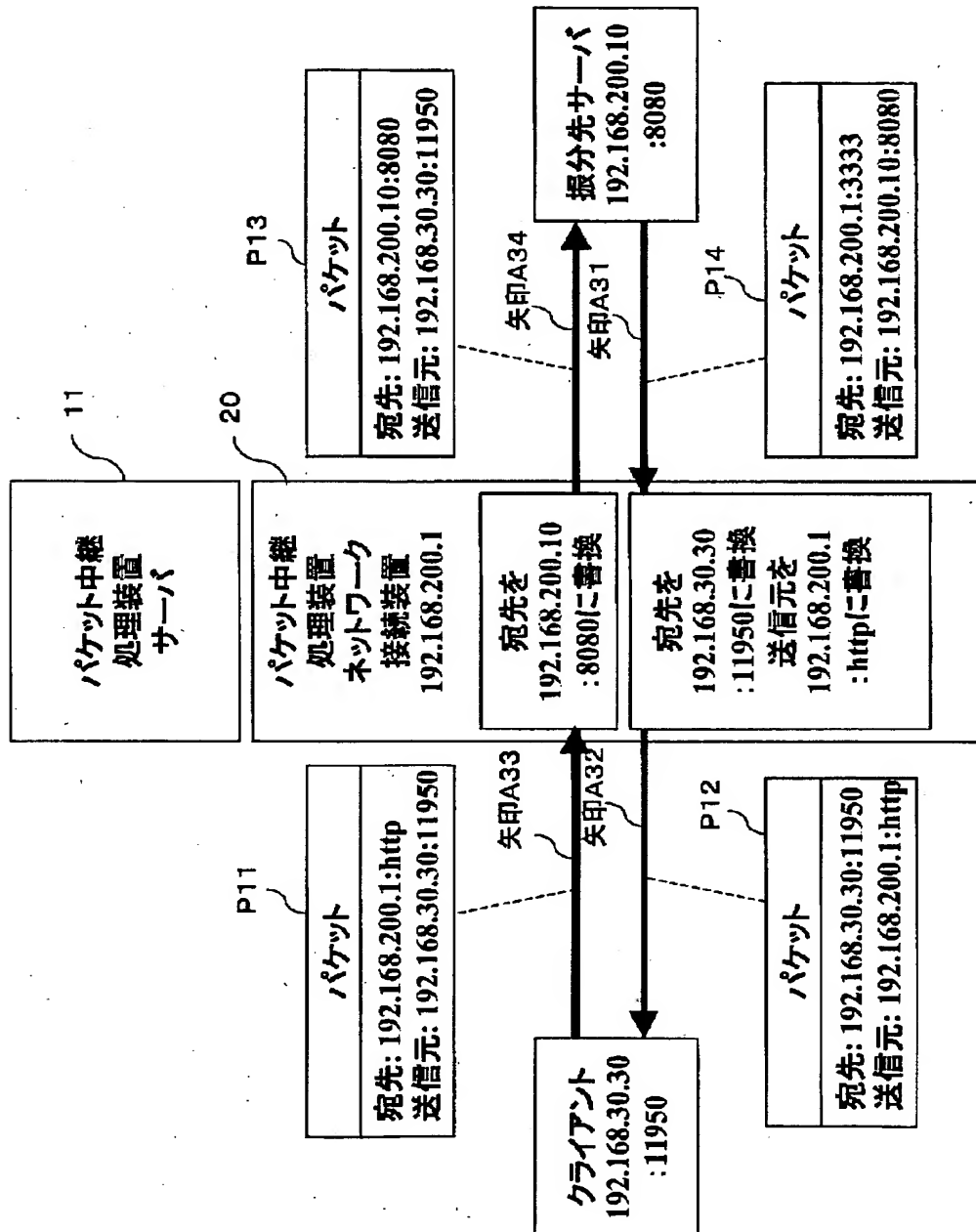
【図 33】

第5実施例におけるURL負荷分散サービスの
パケットフローを示す図(詳細解析前)



【図 34】

第5実施例におけるURL負荷分散サービスの
パケットフローを示す図(詳細解析後)



【図 3 5】

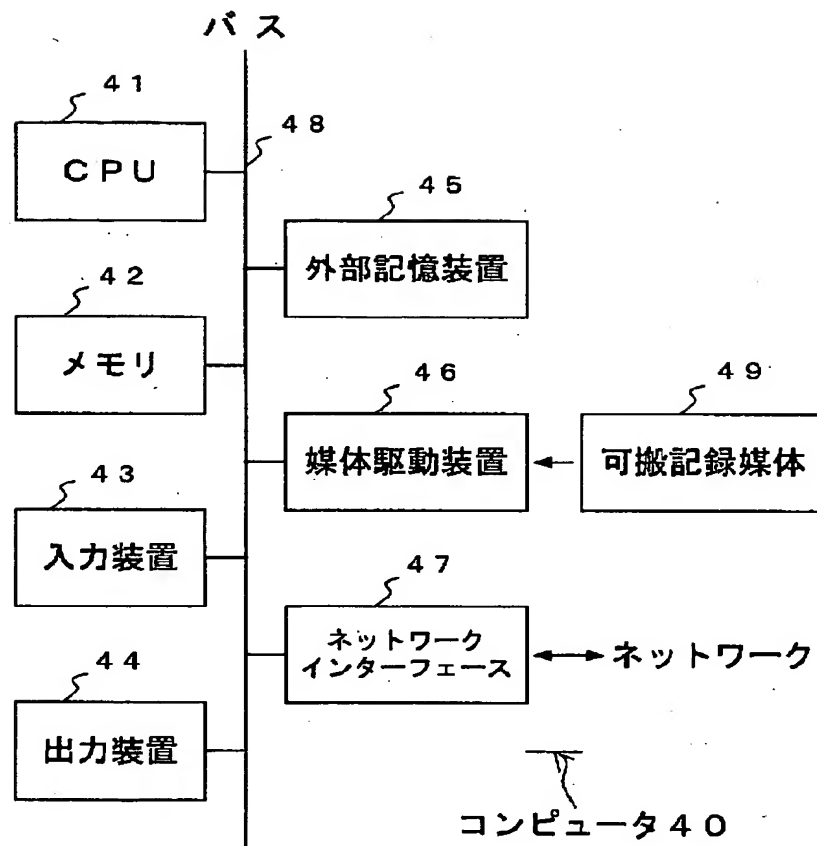
フラグテーブルのデータ構造の一例を示す図

グループID	フラグ
0	0
1	0
2	1
⋮	⋮
255	0

1 : 有効, 0 : 無効

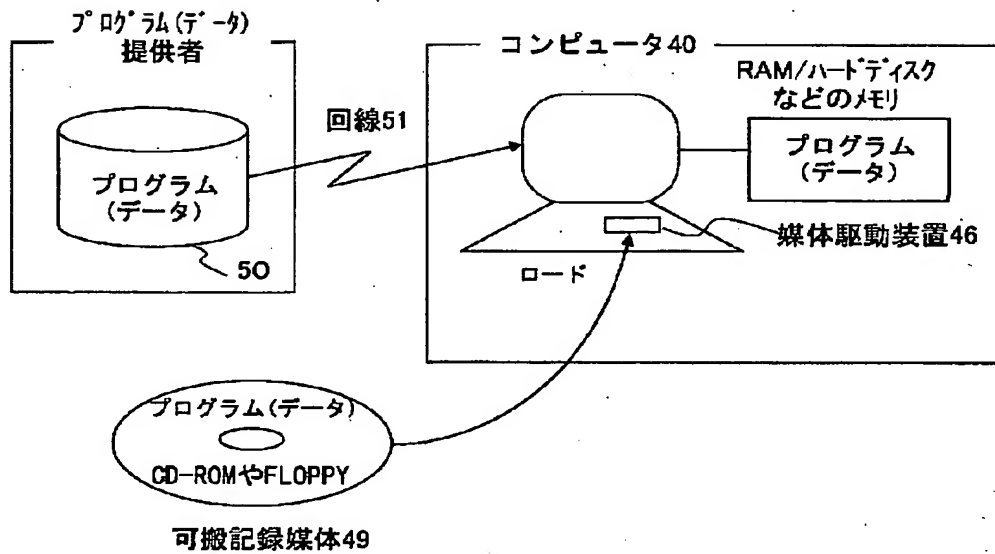
【図36】

コンピュータの構成図



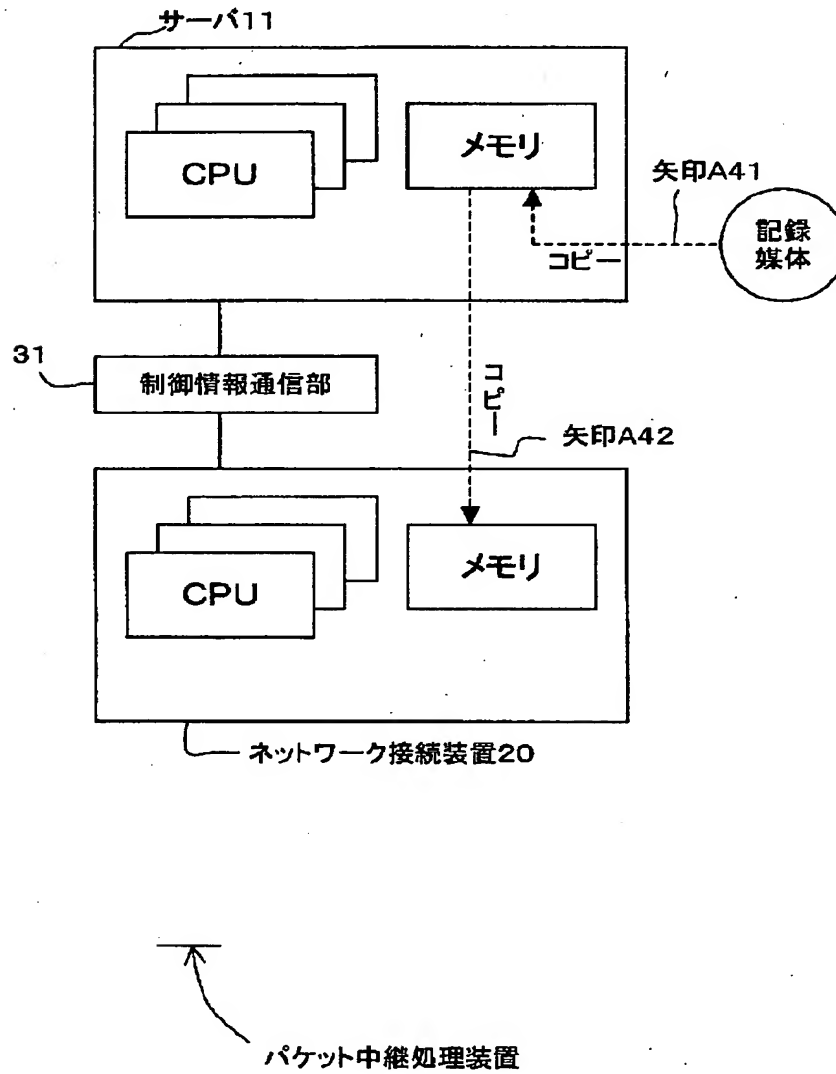
【図37】

コンピュータにプログラムやデータを供給する
記録媒体や伝送記号を説明する図



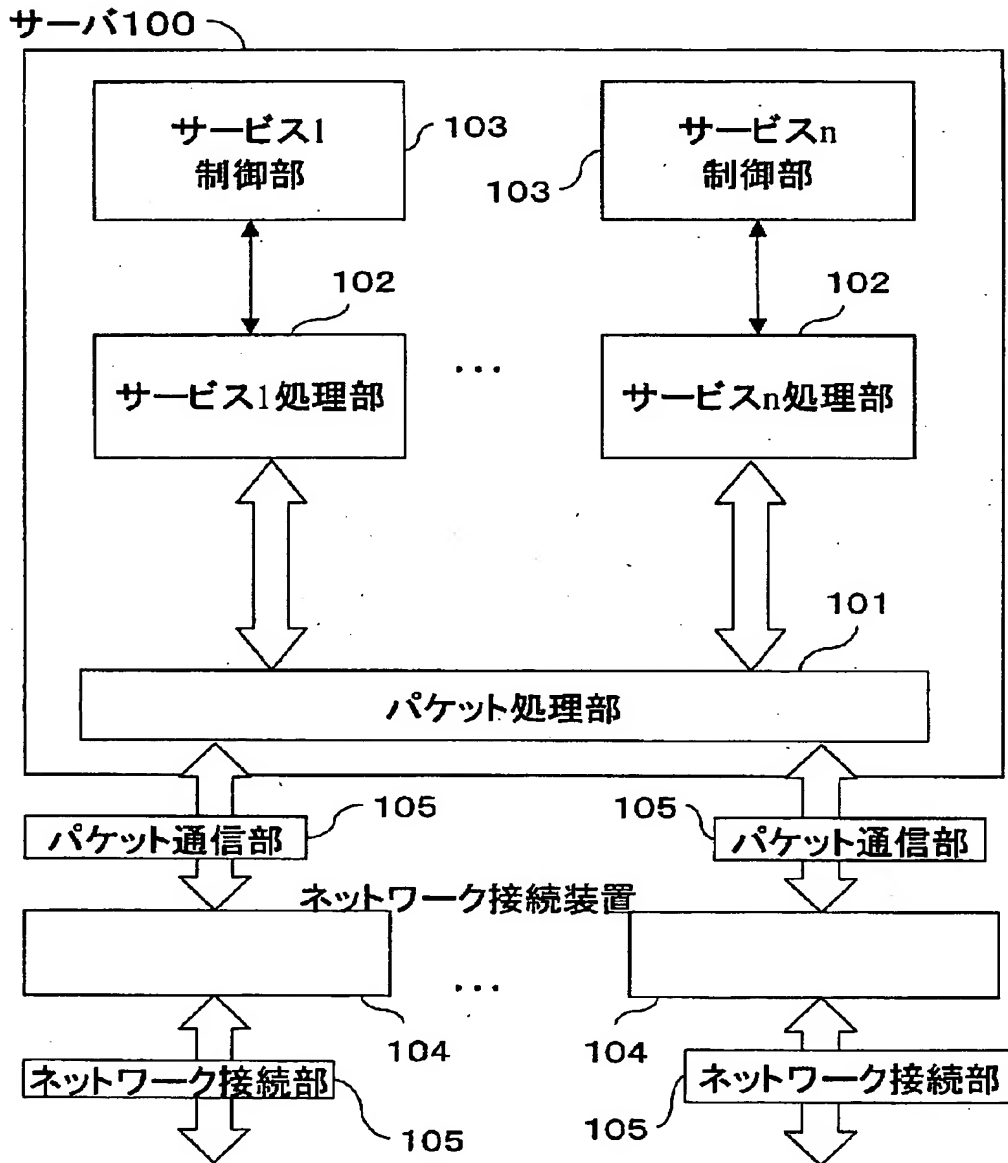
【図 38】

サーバ及びネットワーク接続装置への
プログラムやデータのローディングを説明する図



【図 39】

従来のパケット中継処理装置の構成を示す図



【書類名】 要約書

【要約】

【課題】 多くのネットワークサービスで使用している共通処理を、ネットワーク接続装置に配置することにより、サーバのサービス処理を高速化すること。

【解決手段】 従来サーバ上に配置していたパケット処理部とセッション管理部をネットワーク接続装置 2 上に配置し、ネットワーク接続装置 2 上でセッション管理に基づくパケット中継処理を行う。また、ネットワーク装置 2 上に、処理振分部 2 c とサービス処理部 2 d を設け、サーバ 1 により設定されるポリシーに従って、処理振分部 2 c によりサービス処理部 2 d へのセッション管理に基づく振り分けを行う。さらに、条件に応じてサーバ 1 でセッション管理を行ったり、サーバにもサービス処理を行わせるようにしたり、サーバでパケットを解析してサービス内容を設定し、ネットワーク接続装置が、以後同じセッションに対して上記サービス内容に基づき中継処理を行うようにすることもできる。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号

氏 名 富士通株式会社

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.